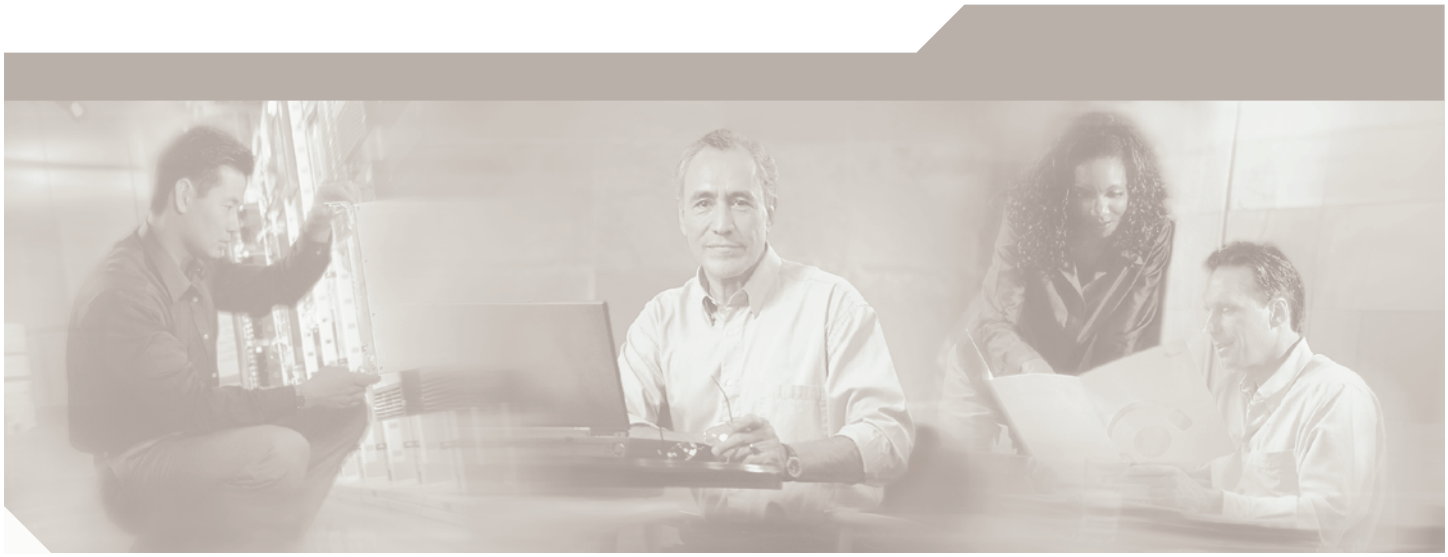
Cisco Systems

Send documentation comments to mdsfeedback-doc@cisco.com



Cisco MDS 9000 Family Fabric and Device Manager User's Guide

Cisco MDS SAN-OS Release 1.3

January, 2004

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Customer Order Number: DOC-7816133=
Customer Order Number: 78-16133-01

CONTENTS

INDEX

New and Changed Information

Table 1 summarizes the new and changed features for the Cisco Fabric Manager Use's Guide/Online Help, and tells you where they are documented. If a feature has changed in release, a brief description of the change appears in the "Description" column, and that release is shown in the "Changed in Release" column.

Table 1 Documented Features for the Fabric Manager User's Guide/Online Help

Feature	Description	Changed in Release	Where Documented
New Installation process	The installation process is slightly different for this release.	1.3(1)	Overview
FM Server	Fabric Manager Server is the server component of Fabric Manager, expanding the capabilities of the product.	1.3(1)	Using Fabric Manager Server
FICON Support	Device Manager now supports FICON management. To use FICON, read the Device Manager and FICON chapters.	1.3(1)	Managing FICON
Inter-VSAN Zoning	Fabric Manager now supports inter-VSAN zones and zonesets.	1.3(1)	Managing Zones and Zonesets
Licensing	Various features now require a license to enable. Refer to the Configuration Guide for a list of these features. The licensing process for Fabric Manager is described in this book.	1.3(1)	Overview
Virtualization	Fabric Manager now recognizes virtual end devices and storage devices.	1.2(2)	Getting Started with Cisco Fabric Manager
Port Security	You can now manage and configure VSAN-based port security using Fabric Manager.	1.2(1a)	Managing Interfaces
IP Filter	You can configure and manage IP profiles and filters using Fabric Manager, to control IP access to a switch.	1.2(1a)	Configuring IP Profiles

Table 1 Documented Features for the Fabric Manager User's Guide/Online Help

Feature	Description	Changed in Release	Where Documented
Common Roles	You can now set the scope of VSAN security with Common Roles, configurable from Fabric Manager or Device Manager.	1.2(1a)	Managing Administrator Access
SPAN	You can now create SPAN sessions and sources with Fabric Manager and Device Manager.	1.2(1a)	Management Services
NTP	You can now create and view NTP peers and servers with Fabric Manager and Device Manager.	1.2(1a)	Management Services
LUN Zoning	You can now allocate (centralize or pool) storage using Fabric Manager.	1.2(1a)	Managing Zones and Zonesets
Read-only Zones	Read-only zones are now configurable and viewable.	1.2(1a)	Managing Zones and Zonesets
DM Summary View	The Device Manager Summary view has been modified.	1.2(1a)	Using Cisco Fabric Manager and Device Manager
Software Upgrade Wizard	A new wizard has been added to the Fabric Manager's Edit menu that allows you to perform software upgrades.	1.2(1a)	Not documented
Show Tech Support	The **show tech support** command can now be run from Fabric Manager on multiple switches simultaneously.	1.2(1a)	Using Cisco Fabric Manager and Device Manager
Opening the Fabric Manager VSAN list	This list is now available from VSAN Attributes under the All VSANs menu.	1.2(1a)	Managing VSANs
Enclosures	You can now create enclosures from the Fabric Manager Information pane, by selecting **Connectivity** > **Storage** from the menu tree of the **Physical** tab. Prior to Release 1.1(1a), you created enclosures by right-clicking on a map object and selecting **Enclosures** from the pop-up menu.	1.1(1a)	Using Cisco Fabric Manager and Device Manager

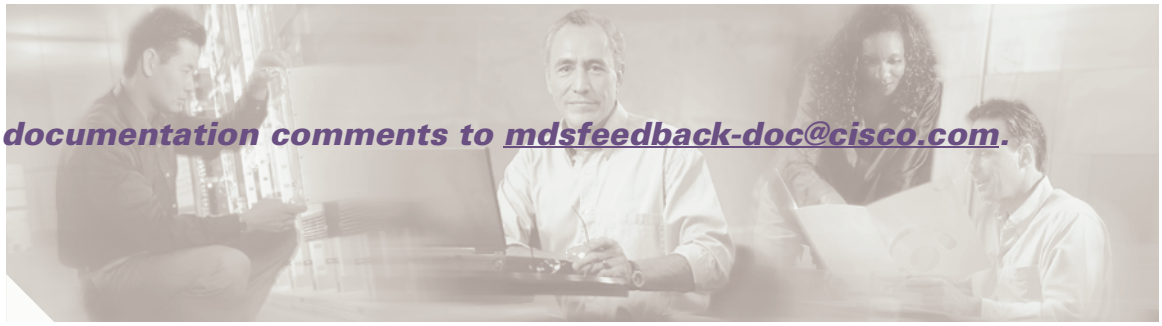
Table 2 contains the history of the changes to the *Cisco MDS 9000 Family Fabric Manager User's Guide/Online Help*, Release 1.3(1). When the document is updated for the next release, these changes are incorporated into the new revision and will no longer appear in this table.

Table 2 Documentation Changes for Fabric Manager User's Guide/Online Help, Release 1.2(2)

Date	Description of Change	Where Changed
10/20/2003	Document Created	---

Send documentation comments to mdsfeedback-doc@cisco.com.

Send documentation comments to mdsfeedback-doc@cisco.com.



Preface

This preface describes the audience, organization, and conventions of the *Cisco MDS 9000 Family Fabric Manager User's Guide*. It also provides information on how to obtain related documentation.

Audience

This guide is for system administrators who intend to use the Cisco Fabric Manager to configure and monitor the switches that build the network fabric.

You should be familiar with the basic concepts and terminology used in internetworking, and understand your network topology and the protocols that the devices in your network can use. You should also have a working knowledge of the operating system on which you are running Fabric Manager, such as Microsoft Windows, Linux, or Solaris.

Organization

This guide contains procedural and conceptual information. For reference information (such as field descriptions for the windows and dialog boxes) refer to the *Cisco MDS 9000 Family Fabric Manager Online Help*. This is accessible by clicking **Help** from the Fabric Manager or Device Manager menus. This guide is organized as follows:

Chapter	Title	Description
Chapter 1	Getting Started with Cisco Fabric Manager	Provides an overview of the Cisco Fabric Manager, Device Manager, Fabric Manager Server, and Performance Manager, and tells how install them.
Chapter 2	Using Fabric Manager Server	Provides an overview of Fabric Manager Server.
Chapter 3	Using Fabric Manager Client	Provides an overview of Fabric Manager Client.
Chapter 4	Using Device Manager	Provides an overview of Device Manager
Chapter 5	Using Performance Manager	Provides an overview of, and describes how to use Performance Manager.
Chapter 6	Managing the System and Components	Describes how to perform system- and component-specific tasks.

Chapter	Title	Description
Chapter 7	Managing VSANs	Describes how to configure VSANs (virtual storage area networks).
Chapter 8	Managing Interfaces	Describes how to view and configure physical port interfaces and Port Channels.
Chapter 9	Managing Zones and Zone Sets	Describes how to configure zones and zone sets.
Chapter 10	Managing Administrator Access	Describes how to perform administrative tasks.
Chapter 11	Managing IP Storage	Describes how to configure FCIP and iSCSI storage services.
Chapter 12	Managing IP Services	Describes how to configure all other IP storage services.
Chapter 13	Managing FICON	Describes how to configure and manage FICON services.
Chapter 14	Troubleshooting the Fabric	Describes how to use Fabric Manager to get information about your switches and fabrics.
Chapter 15	Troubleshooting Fabric Manager Issues	Describes how to troubleshoot various issues with Fabric Manager.
Chapter 16	Managing Advanced Features	Describes how to configure advanced features, including: • World wide names • Domain parameters • Name server

Conventions

This guide uses the following conventions:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Caution Means *reader be careful*. In this situation, you might do something that could result in loss of data.

Send documentation comments to

Related Documentation

For Fabric Manager and Device Manager field descriptions, refer to the *Cisco MDS 9000 Family Fabric Manager Online Help*. For additional information, refer to the following documents:

- *Regulatory Compliance and Safety Information for the Cisco MDS 9000 Family*
- *Cisco MDS 9100 Series Hardware Installation Guide*
- *Cisco MDS 9200 Series Hardware Installation Guide*
- *Cisco MDS 9500 Series Hardware Installation Guide*
- *Cisco MDS 9000 Family Configuration Guide*
- *Cisco MDS 9000 Family Command Reference*
- *Cisco MDS 9000 Family Troubleshooting Guide*
- *Cisco MDS 9000 Family System Messages Guide*
- *Cisco MDS 9000 Family MIB Reference Guide*

For information on VERITAS Storage Foundation™ for Networks 1.0, *Cisco* software, refer to the following Veritas documents available at http://support.veritas.com/:

- *VERITAS Storage Foundation for Networks Overview*
- *VERITAS Storage Foundation for Networks Installation and Configuration Guide*
- *VERITAS Storage Foundation for Networks Obtaining and Installing Licenses*
- *VERITAS Storage Foundation for Networks GUI Administrator's Guide*
- *VERITAS Storage Foundation for Networks CLI Administrator's Guide*
- *VERITAS Storage Foundation for Networks README*

For information on IBM SAN Volume Controller Storage Software for Cisco MDS 9000, refer to the following IBM documents available on the IBM TotalStorage Support web site: http://www.ibm.com/storage/support/2062-2300

- *IBM TotalStorage SAN Volume Controller Storage Software for Cisco MDS 9000 - Getting Started*
- *IBM TotalStorage SAN Volume Controller Storage Software for Cisco MDS 9000 - Configuration Guide*
- *IBM TotalStorage SAN Volume Controller Storage Software for Cisco MDS 9000 - Supported Hardware List*
- *IBM TotalStorage SAN Volume Controller Storage Software for Cisco MDS 9000 -Supported Software Levels*
- *IBM TotalStorage SAN Volume Controller Storage Software for Cisco MDS 9000 - Command Line Interface User's Guide*
- *IBM TotalStorage SAN Volume Controller Storage Software - Host Attachment Guide*
- *Subsystem Device Driver User's Guide*

Send documentation comments to

Obtaining Documentation

These sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com

Translated documentation is available at this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Ordering Documentation

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. In the Cisco Documentation home page, click the **Fax** or **Email** option in the “Leave Feedback” section at the bottom of the page.

You can e-mail your comments to mdsfeedback-doc@cisco.com.

You can submit your comments by mail by using the response card behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

Send documentation comments to

We appreciate your comments.

Obtaining Technical Assistance

Note If you purchased this product through a Cisco reseller, contact the reseller directly for technical support. If you purchased this product directly from Cisco, contact Cisco Technical Support at this URL: http://www.cisco.com/warp/public/687Directory/DirTAC.shtml

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

If you want to obtain customized information and service, you can self-register on Cisco.com. To access Cisco.com, go to this URL:

http://www.cisco.com

Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Cisco TAC inquiries are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

The Cisco TAC resource that you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

You can use the Cisco TAC Web Site to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

http://www.cisco.com/register/

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC Web Site, you can open a case online by using the TAC Case Open tool at this URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

Send documentation comments to

CHAPTER 1

Getting Started with Cisco Fabric Manager

The Cisco Fabric Manager is a set of network management tools that supports Secure Simple Network Management Protocol version 3 (SNMPv3) and legacy versions. It provides a graphical user interface (GUI) that displays real-time views of your network fabric, and lets you manage the configuration of Cisco MDS 9000 Family devices and third-party switches. The Cisco Fabric Manager applications are:

- Fabric Manager Server
- Device Manager
- Fabric Manager Client
- Performance Manager

Fabric Manager Server is the server component of the Cisco Fabric Manager tool set, and must be started before running Fabric Manager. On a Windows PC, Fabric Manager Server is installed as a service. This service can then be administered using the Service Panel in the Control Panel.

The Fabric Manager displays a map of your network fabric, including Cisco MDS 9000 Family switches, third-party switches, hosts, and storage devices.

The Device Manager presents two views of a switch.

- Device View displays a graphic representation of the switch configuration, and provides access to statistics and configuration information for a single switch.
- Summary View displays a summary of xEPorts (Inter-Switch Links), Fx Ports (fabric ports), and Nx Ports (attached hosts and storage) on the switch, as well as FC and IP neighbor devices.

Performance Manager provides detailed traffic analysis by capturing data with SNMP. This data is compiled into various graphs and charts which can be viewed with any web browser.

The Cisco Fabric Manager applications are an alternative to the command-line interface (CLI) for most switch configuration commands. For information on using the CLI to configure a Cisco MDS 9000 Family switch, refer to the *Cisco 9000 Family Configuration Guide* or the *Cisco 9000 Family Command Reference*.

To learn more about the general capabilities of Cisco Fabric Manager, refer to the following topics:

- Managing Cisco MDS 9000 Switches, page 1-2
- Storage Management Solutions Architecture, page 1-3
- In-Band Management and Out-of-Band Management, page 1-4

For licensing information, refer to the following topic:

- Cisco MDS 9000 Family Licensing, page 1-4

To learn about installing and accessing Fabric Manager and Device Manager on your system, refer to the following topic:

- Installing the Applications, page 1-6
- Launching the Applications, page 1-8
- A Note on Ports, page 1-8

For detailed information about Fabric Manager Server, Fabric Manager, and Device Manager, refer to the following topics:

- Chapter 2, “Using Fabric Manager Server”
- Chapter 3, “Using Fabric Manager Client”
- Chapter 4, “Using Device Manager”
- Chapter 5, “Using Performance Manager”

Managing Cisco MDS 9000 Switches

The Cisco MDS 9000 Family of switches can be accessed and configured in many different ways, and support standard management protocols. The different protocols that are supported in order to access, monitor, and configure the Cisco MDS 9000 Family of switches are described in Table 1-1.

Table 1-1 Supported Management Protocols

Management Protocol	Purpose
Telnet/SSH	Provides remote access to the CLI for a Cisco MDS 9000 switch.
FTP/SFTP/TFTP, SCP	Copies configuration and software images between devices.
SNMPv1, v2c, and v3	Includes over 70 distinct Management Information Bases (MIBs). Cisco MDS 9000 Family switches support SNMP version 1, 2, and 3 and RMON V1 and V2. RMON provides advanced alarm and event management, including setting thresholds and sending notifications based on changes in device or network behavior. By default, the Cisco Fabric Manager communicates with Cisco MDS 9000 Family switches using SNMPv3, which provides secure authentication using encrypted user names and passwords. SNMPv3 also provides the option to encrypt all management traffic.
HTTP	HTTP is only used for the distribution and installation of the Cisco Fabric Manager software. It is *not* used for communication between the Cisco Fabric Manager and Cisco MDS 9000 Family switches.

Table 1-1 Supported Management Protocols

Management Protocol	Purpose
ANSI T11 FC-GS3	Fibre Channel-Generic Services (FC-GS)3 in the definition of the management servers defines the Fabric Configuration Server (FCS), which is a standard mechanism to collect information about platforms (end devices) and interconnecting elements (switches) building the fabric. The Cisco MDS 9000 uses the information provided by FCS on top of the information contained in the Name Server database and in the Fibre Channel Shortest Path First (FSPF) topology database to build a detailed topology view, and collect information for all the devices building the fabric.
XML/CIM	CIM server support for designing storage area network management applications to run on Cisco MDS SAN-OS.

Storage Management Solutions Architecture

Management services required for the storage environment can be divided into five “layers,” with the bottom layer being closest to the physical storage network equipment, and the top layer managing the interface between applications and storage resources.

Of these five layers of storage network management, Cisco Fabric Manager provides tools for device (element) management and fabric management. In general, the Device Manager is most useful for device management (a single switch), while Fabric Manager is more efficient for performing fabric management operations involving multiple switches.

Tools for “upper-layer” management tasks can be provided by Cisco or by third-party storage and network management applications. The following summarizes the goals and function of each layer of storage network management:

- Device management provides tools to configure and manage a device within a system or a fabric. You use device management tools to perform tasks on one device at a time, such as initial device configuration, setting and monitoring thresholds, and managing device system images or firmware.
- Fabric management provides a system-oriented view of a fabric and its devices. Fabric management applications provide fabric discovery, fabric monitoring, reporting, and fabric configuration.
- Resource management provides tools for managing resources such as fabric bandwidth, connected paths, disks, I/O operations per second (IOPS), CPU, and memory. You can use Fabric Manager to perform some of these tasks.
- Data management provides tools for ensuring the integrity, availability, and performance of data. Data management services include redundant array of independent disks (RAID) schemes, data replication practices, backup or recovery requirements, and data migration. Data management capabilities are provided by third-party tools.
- Application management provides tools for managing the overall system consisting of devices, fabric, resources, and data from the application. Application management integrates all these components with the applications that use the storage network. Application management capabilities are provided by third-party tools.

In-Band Management and Out-of-Band Management

Cisco Fabric Manager requires an out-of-band (Ethernet) connection to at least one Cisco MDS 9000 Family switch. You need either mgmt0 or IP over Fibre Channel (IPFC) to manage the fabric.

MGMT0

The interface referred to as the out-of-band management connection is a 10/100 Mbps Ethernet interface on the supervisor module, labeled mgmt0. The mgmt0 interface can be connected to a management network to access the switch through IP over Ethernet. You must connect to at least one Cisco MDS 9000 Family switch in the fabric, through its Ethernet management port. You can then use this connection to manage the other switches using in-band (Fibre Channel) connectivity. Otherwise, you need to connect the mgmt0 port on each switch to your Ethernet network.

Each supervisor module has its own Ethernet connection; however, the two Ethernet connections in a redundant supervisor system operate in active or standby mode. The active supervisor module also hosts the active mgmt0 connection. When a failover event occurs to the standby supervisor module, the IP address and media access control (MAC) address of the active Ethernet connection are moved to the standby Ethernet connection.

IPFC

You can also manage switches on a Fibre Channel network using an in-band IP connection. The Cisco MDS 9000 Family supports RFC 2625 IP over Fibre Channel, which defines an encapsulation method to transport IP over a Fibre Channel network.

IPFC encapsulates IP packets into Fibre Channel frames so that management information can cross the Fibre Channel network without requiring a dedicated Ethernet connection to each switch. IP addresses are resolved to the Fibre Channel address through Address Resolution Protocol (ARP). This feature allows you to build a completely in-band management solution.

Cisco MDS 9000 Family Licensing

From Release 1.3(x), the SAN-OS software requires licenses in all switches in the Cisco MDS 9000 Family. The licensing functionality allows you to access specified premium features on the switch after you install the appropriate license for that feature. You need a license:

- For each switch managed by a Fabric Manager server
- If you are upgrading from 1.2(x) to 1.3 and you are using Enterprise or FCIP

For information on license installation and license management using Fabric Manager and Device Manager, refer to the following topics:

- Installing Licenses, page 1-5
- Viewing License Information, page 1-5
- Removing Licenses, page 1-6

For more information on the licensing model, license concepts, and license installation and management using the CLI, refer to the *Cisco MDS 9000 Configuration Guide*.

Note If you purchased your Cisco MDS 9000 switch through a Cisco reseller, contact the reseller directly for technical support. If you purchased this product directly from Cisco, contact Cisco Technical Support at this URL: http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Caution The feature-based license for your switch is tied to the supervisor module and the serial number of your switch. (Module-based licenses are specific to each module and can be moved between switches.) If you move a supervisor module to another switch, your license will no longer work. You will need to contact technical support to obtain a new license for the new switch/supervisor combination.

Similarly, if you RMA a chassis you will need to obtain a new license for the replacement chassis.

Installing Licenses

If you have purchased a new switch through either your reseller or through Cisco, you can have the licenses pre-installed in the factory, or you can install the licenses yourself. If you already have an existing switch, you install the licenses yourself. The best way to install licenses on the switches in your fabric is to use the One Click Install provided by the License Manager in Fabric Manager. You can also use Device Manager to install licenses on each switch individually.

Note You do not need a license to access a switch with Fabric Manager. Refer to the *Cisco MDS 9000 Family Configuration Guide* for a list of features requiring licenses.

To install the licenses, perform the following procedure:

Step 1 Log into a switch in the fabric containing the switches for which you want to install licenses. To install licenses on multiple switches, you do not need to log into each switch; however, the switch must be in the fabric you are viewing.

Step 2 From Fabric Manager, select Switches -> License Manager from the Physical pane. The license information is displayed in the Information pane, one line per feature. Click the File tab, and then click the Create Row button in the toolbar. The License Manager Fetch and Install Licenses dialog is displayed.

Step 3 Check the checkboxes in the Select column for each switch on which you are installing a license.

Step 4 For each switch you have checked, enter the PAK in the PAK field for that switch.

Step 5 Enter the file name for the License Key File in the Filename field.

Step 6 Select the protocol you want to use to access the Cisco license web site.

Step 7 Click the Install License button.

Fabric Manager accesses the Cisco license site and installs the licenses onto each switch.

Note If you have purchased your Cisco MDS 9000 switch through a Cisco reseller, contact the reseller directly for information on accessing their license web site.

Viewing License Information

To view license information in Fabric Manager, perform these steps:

Step 1 Select Switches -> License Manager from the Physical pane. The license information is displayed in the Information pane, one line per feature.

Step 2 Click the Feature Usage tab to see the Switch, name of the feature package, the type of license installed, the number of licenses used (Usage Count), the expiration date, the grace period (if you do not have a license for a particular feature), and any errors (e.g., if you have a missing license). Click the File tab to display the information about each of the License Key Files installed on your switch.

Caution Once an expiration period has started, notifications about license expiration appear in the Fabric Manager's Events pane on a daily basis. During the last seven days of the expiration period, these messages are displayed hourly. After the final seven days of the expiration period, the feature is turned off and your network traffic may be disrupted.

To view license information in Device Manager, perform these steps:

Step 1 Select License Manager from the Admin menu. The License Manager dialog is displayed.

Step 2 Click the Features tab to see the name of the feature package, the type of license installed, the number of licenses used (Usage Count), the expiration date, the grace period (if you do not have a license for a particular feature), and any errors (e.g., if you have a missing license). Click the Files tab to display the information about each of the License Key Files installed on your switch.

Removing Licenses

To remove the licenses, perform the following procedure:

Step 1 Log into the switch. If you are using Fabric Manager to remove licenses from multiple switches, you do not need to log in to each switch; however, the switches must be in the fabric you are viewing.

Step 2 From Fabric Manager, select Switches -> License Manager from the Physical pane. The license information is displayed in the Information pane, one line per feature.

From Device Manager, select License Manager from the Admin menu. The License Manager dialog is displayed.

Step 3 In Fabric Manager, click the File tab. The list of License Key Files is displayed. Click on the Name of the license you want to remove, and press the Delete key or click on the Delete Row icon in the toolbar.

In Device Manager, click Uninstall, and enter the name of the License Key File you want to remove. Click Apply to remove the License Key File, and click Close to close the dialog.

Note To delete a license, you must disable the features enabled by that license. The delete procedure fails if the license is in use, and an error message is displayed.

Installing the Applications

Before you can access the Cisco Fabric Manager, you must complete the following tasks:

- A supervisor module must be installed on each switch that you want to manage.
- The supervisor module must be configured with the following values using the setup routine or the CLI:
  - IP address assigned to the mgmt0 interface
  - SNMP Credentials (v1/v2 communities, or v3 user name and password), maintaining the same password for all the switches in the fabric. Must be on each PC.

The Cisco Fabric Manager software executables reside on each supervisor module of each Cisco MDS 9000 Family switch in your network. The supervisor module provides an HTTP server that responds to browser requests and distributes the software to Windows or UNIX network management stations.

To install the software for the first time, or if you want to update or reinstall the software, access the supervisor module with a web browser. When you click the Install buttons on the web page that is displayed, the software running on your workstation is verified to make sure you are running the most current version of the software. If it is not current, the most recent version is downloaded and installed on your workstation.

New installation options include:

- Upgrade/Downgrade - The installer detects your current version of Fabric Manager and Device Manager, and provides the option to upgrade or downgrade. The default is to upgrade to the latest version of Fabric Manager or Device Manager.
- Autoupgrade - If you always want to run the latest version of Fabric Manager and Device Manager, select "Always autoupgrade, don't ask me again." Subsequent upgrades will happen automatically, without prompting.
- Uninstall - Before upgrading or uninstalling Fabric Manager or Device Manager, make sure any instances of these applications have been shut down. Use the Uninstall batch file or shell script to uninstall. Do not delete the .cisco_mds9000 folder as this might make your installation unsafe for upgrades.

To download and install the software on your workstation, follow these steps:

Step 1 Enter the IP address or host name of the supervisor module in the address or location field of your browser.

When you connect to the server for the first time, it checks to see if you have the correct Sun Java Virtual Machine version installed on your workstation. If not, a link is provided to the appropriate web page on Sun Microsystem's website so you can install it.

The supervisor module HTTP server displays the window.

Step 2 Click the link to the Sun Java Virtual Machine software (if required) and install the software.

Using the instructions provided by the Sun Microsystems website to reconnect to the supervisor module by reentering the IP address or host name in the Location or Address field of your browser.

Note The recommended version of Java is 1.4.2, although 1.4 and above is supported. To change the JRE version, start Java Web Start and set the Java preferences.

Step 3 Click on any installation link (**Fabric Manager** or **Device Manager**).

You see a prompt asking for permission to install the applications on your workstation.

Clicking on a link first runs an installer, which detects the installed version of the software, prompts for upgrades/downgrades and other options if applicable, and runs the application you selected.

All software is installed in a folder called ".cisco_mds9000". On a Windows machine, the pathname is %HOME%\.cisco_mds9000. On a UNIX machine, the pathname is $HOME/.cisco_mds9000.

On a Windows machine, a "Cisco MDS" program group is created under Start->Programs. This program group contains shortcuts to batch files in the install directory. On a Solaris or Linux machine, shell scripts are created in the install directory.

Note Fabric Manager cannot run without the server component, Fabric Manager Server. Fabric Manager Server is downloaded and installed when you download and install Fabric Manager or Device Manager. On a Windows machine you install the FMServer as a service. This service can then be administered using the Service Panel in the Control Panel. The default setting for the FMServer service is that the server is automatically started when the machine is rebooted. You can change this behavior by modifying the properties in the Service panel.

Launching the Applications

To launch the Fabric Manager Server, Fabric Manager Client (Fabric View) or Device Manager (Device View and Summary View), follow these steps:

Step 1 Double-click the **Fabric Manager** icon or the **Device Manager** icon on your desktop or select the option from the Windows Start menu.

If you double-clicked on Fabric Manager, the Fabric Manager Server will load (a command line window will appear briefly).

A log-in screen for Fabric Manager or Device Manager is displayed.

Step 2 Enter the IP address or device name in the Device Name(s) field, or select an IP address from the list of previously accessed devices, accessible through the drop-down arrow to the right of the Device Name(s) field.

Step 3 Check the SNMPv3 check box to select SNMP version 3.

Note The default authentication digest used for storing user names and passwords is MD5. In case you selected SHA instead, the relative checkbox in the Fabric Manager initial login screen should be checked.

Step 4 Enter a user name and password.

Step 5 If the SNMPv3 Privacy option is enabled, enter the Privacy Password used for encrypting management traffic

The Privacy option causes all management traffic to be encrypted while, with SNMPv3, user names and passwords are always encrypted.

To enable the Privacy option, see Chapter 10, “Managing Administrator Access.”

Step 6 Click **Open**.

You see either the Fabric Manager or the Device Manager.

A Note on Ports

For PCs running Fabric Manager Server, Fabric Manager Client, Device Manager, and Performance Manager, certain ports need to be available.

Fabric Manager Client and Device manager use the first available UDP port for receiving SNMP responses. The UDP SNMP Trap local ports are (FM=1162, DM=1163 or 1164). Fabric Manager Client also opens TCP RMI port (9099). If Device Manager is opened from Fabric Manager Client, it listens on the first available UDP port for Fabric Manager requests.

CHAPTER 2

Using Fabric Manager Server

Fabric Manager cannot run without the server component, Fabric Manager Server. Fabric Manager Server provides:

- Multiple physical fabric management
- Centralized fabric discovery services
- Continuous MDS health and event monitoring
- Long term historical Fibre Channel Performance data collection
- Performance reports and charting for hotspot analysis

When you click on the Fabric Manager icon, the dialog box allows you to enter the IP address of a switch containing the Fabric Manager Server. If the server is running on your local machine, leave "localhost" in that field. If you try to run Fabric Manager without specifying a valid server, you are prompted to start the FMServer.

On a Windows PC, you install the FMServer as a service. This service can then be administered using the Service Panel in the Control Panel. The default setting for the FMServer service is that the server is automatically started when the machine is rebooted. You can change this behavior by modifying the properties in the Service panel.

Note If your computer has multiple interface cards (NICs), choose a local interface that can reach Fibre Channel network on clients and on the server.

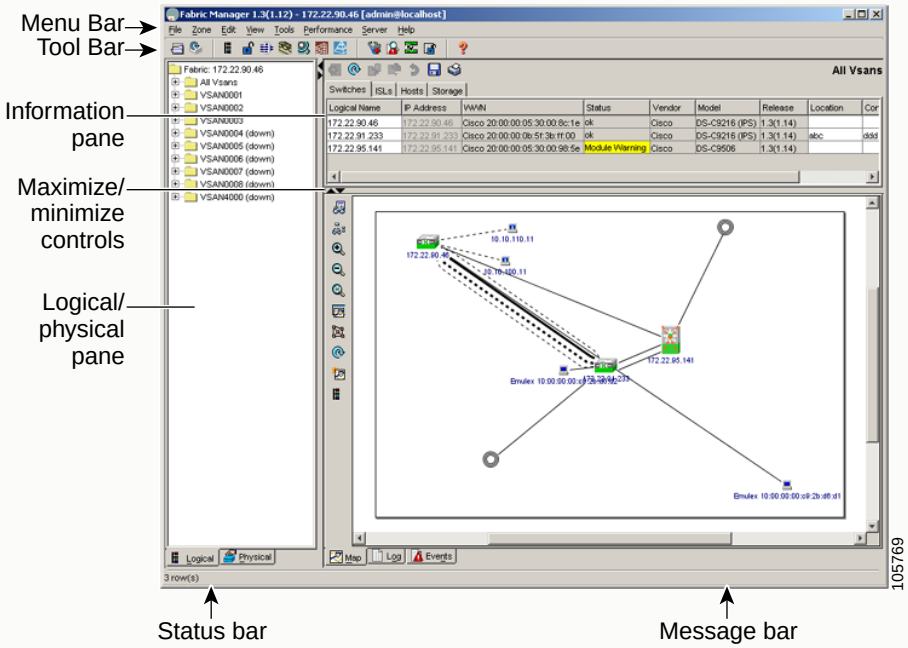
CHAPTER 3

Using Fabric Manager Client

The Fabric Manager displays a view of your network fabric, including Cisco MDS 9000 or third-party switches and end devices. To launch the Fabric Manager from your desktop, double-click the **Fabric Manager** icon and follow the instructions described in the "Launching the Applications" section on page 1-8. Figure 3-1 shows the Fabric Manager main window.

Note Changes made using Fabric Manager are applied to the running configuration of the switches you are managing and the changes may not be saved when the switch restarts. After you make a change to the configuration or perform an operation (such as activating zones), the system prompts you to save your changes before you exit.

Figure 3-1 Fabric Manager Main Window



The menu bar at the top of the Fabric Manager window provides access to options, that are organized by menus. The toolbar provides icons that duplicate the most commonly used options on the File, Tools, and Help menus.

The main window has a menu bar, toolbar, message bar, status bar, and three panes:

- Logical/Physical pane—Displays a tree of configured VSANs and zones on the Logical tab and a menu tree of available configuration tasks on the Physical tab.
- Information pane—Displays information about whatever option is selected in the menu tree.
- Map pane—Displays a map of the network fabric, including switches, hosts, and storage. It also provides tabs for displaying log and event data.

You can resize each pane by dragging the boundaries between each region or by clicking the **Minimize** or **Maximize** controls. (See Figure 3-1.)

Menu Bar, Toolbars, and Message Bar

The menu bar at the top of the Fabric Manager window provides options for managing and troubleshooting the current fabric and for controlling the display of information on the Map pane. The menu bar provides the following menus:

- File—Open a new fabric, rediscover the current fabric, locate switches, set preferences, print the map, and clear or export the Map pane log.
- Zone—Manage zones, zonesets, and various elements on the Fabric Manager map.

- Edit—Allows you to find objects on the Fabric Manager map, or launches the four Fabric Manager wizards - Port Channel, FCIP Tunnel, IP Filter, and Software Upgrade. (You can also launch these wizards from the Fabric Manager toolbar.)
- View—Change the appearance of the map (these options are duplicated on the Map pane toolbar).
- Tools—Verify and troubleshoot connectivity and configuration, as described in the "Analyzing Switch Fabric Configuration" section on page 14-2.
- Performance—Run Performance Manager and Cisco Traffic Analyzer, and generate reports.
- Server—Run administrative tasks on clients and fabrics.
- Help—Display online help topics for specific dialog boxes in the Information pane.

The Fabric Manager main toolbar provides buttons for accessing the most commonly used menu bar options. The Map pane toolbar provides buttons for managing the appearance of the map. The Information pane toolbar provides buttons for editing and managing the Information pane.

The message bar shows the last entry displayed by the discovery process, and the possible error message. It displays a dialog stating that something has changed in the fabric and a new discovery is needed. The status bar shows both short-term, transient messages (such as the number of rows displayed in the table), and long-term discovery issues.

Logical/Physical Pane

Use the **Logical** tab on the **Logical/Physical** pane to manage virtual SAN attributes (e.g., zones) in the currently discovered fabric. For information about managing VSANs see Chapter 7, "Managing VSANs."

To manage zones, right-click one of the folders in the VSAN tree and click **Edit Local Zone Database** from the pop-up menu. You see the **Edit Local Zone Database** dialog box. For information about managing zones and zone sets, see Chapter 9, "Managing Zones and Zone Sets."

Use the **Physical** tab on the **Logical/Physical** pane to display a menu tree of the options available for managing the switches in the currently discovered fabric.

To select an option, click a folder to display the options available and then click the option. You see the dialog box for the selected option in the Information pane. The menu tree provides the following main folders:

- Switches—View and configure hardware components, ports, and PortChannel interfaces.
- FC—View and configure Fibre Channel network configurations.
- IP—View and configure IP storage and IP services.
- Events—View and configure events, alarms, thresholds, notifications, and informs.
- Security—View and configure control and non-VSAN datapath security.
- Connectivity—View and configure ISLs, Hosts, and Storage components.

Information Pane

The Information pane displays tables or other information associated with the option selected from the menu tree. The Information pane toolbar provides buttons for performing one or more of the following operations:

- Apply Changes—Apply configuration changes.
- Refresh Values—Refresh table values.

- Copy…Ctrl+C — Copy data from one row to another.
- Paste…Ctrl +V—Paste the data from one row to another.
- Undo Changes…Ctrl-Z—Undo the most recent change.
- Export—Export and save information to a file.
- Print Table —Print the contents of the Information pane.

Note After making changes you must save the configuration or the changes will be lost when the device is restarted.

Note The buttons that appear on the toolbar vary according to the option you select. They are activated or deactivated (grayed) according to the field or other object that you select in the Information pane.

Map Pane

The Map pane shows the graphical representation of your fabric. Table 3-1 explains the graphics you may see displayed, depending on which devices you have in your fabric.

Table 3-1 Fabric Manager Graphics

Icon or Graphic	Description
	Director Class MDS 9000
	Non-director Class MDS 9000
	Generic FC Switch
	Cisco SN5428
	A line through a device indicates that the device is not manageable
	An "X" through a device or link indicates that the device is down or that the connection is down
	FC HBA (or enclosure)
	FC Target (or enclosure)
	iSCSI Host
	Fibre Channel ISL and Edge
	Fibre Channel Port Channel
	IP ISL and Edge

Icon or Graphic	Description
	IP Port Channel
	FC Loop (Storage)
	IP Cloud (Hosts)
	Any device, cloud, or loop with a box around it means that there are hidden links attached

There are three tabs on the bottom of the Map pane:

- Map—Displays a graphical view of the network fabric with switches, hosts, and storage subsystems.
- Log—Displays messages that describe system operations, such as fabric discovery.
- Events—Displays information about the SNMP traps received by the management station.

When viewing large fabrics in the Map pane, it is helpful to keep the following tips in mind to make the display cleaner.

- Turn off end device labels
- Collapse loops
- Collapse expanded multiple links (collapsed multiple links are shown as very thick single lines)
- Dim or hide portions of your fabric by VSAN

When you right-click an icon, you see a pop-up menu with options that vary depending on the type of icon selected. The various options available for different objects include the following:

- Open an instance of Device Manager for the selected switch.
- Open a CLI session for the selected switch.
- Copy the display name of the selected object.
- Execute a **ping** or **traceroute** command for the device.
- Show or hide end devices.
- Create or delete an enclosure.
- Set the VSAN ID for an edge port (link).
- Set the trunking mode for an ISL.
- Create or add to a PortChannel for selected ISLs.

The Map pane has its own toolbar with options for saving, printing, and changing the appearance of the map. When you right-click on the map, a pop-up menu appears that provides options (duplicated on the toolbar) for changing the appearance of the map.

Note When a VSAN, zone, or zone member is selected in the VSAN tree, the map highlighting changes to identify the selected objects. To remove this highlighting, click the **Clear Highlight** button on the Map pane toolbar or choose **Clear Highlight** from the pop-up menu.

Discovering and Viewing the Network Fabric

Cisco Fabric Manager collects information on the fabric topology, sends SNMP queries to the SNMP agent running on the switch to which Fabric Manager is connected. The switch replies after having discovered all devices connected to the fabric by using the information coming from its FSPF technology database and the Name Server database, and collected using the Fabric Configuration Server's request/response mechanisms defined by the FC-GS3/4 standard. When you start the Fabric Manager, you enter the IP address (or host name) of a "seed" switch.

After you start Fabric Manager and discovery completes, Fabric Manager presents you with a view of your network fabric, including all discovered switches, hosts, and storage devices.

You use the Fabric Manager to discover and view your fabric topology and to manage zones and zone sets. It is also convenient to use the Fabric Manager to manage other kinds of configuration involving more than one switch, such as VSANs and Port Channels.

Controlling Administrator Access with Users and Roles

Cisco MDS 9000 Family switches support role-based management access whether using the CLI or the Cisco Fabric Manager. This lets you assign specific management privileges to particular roles and then assign one or more users to each role.

Cisco Fabric Manager uses SNMPv3 to establish role-based management access. After completing the setup routine, a single role, user name, and password are established. The role assigned to this user allows the highest level of privileges, which includes creating new users and roles. Use the Cisco Fabric Manager to create roles and users, and to assign passwords as required for secure management access in your network.

To enable RADIUS authentication of CLI users or to establish SNMP users and roles, see Chapter 10, "Managing Administrator Access."

Modifying Device Grouping

Because of not all the devices are capable of responding to FC-GS3 requests, different ports of a single server or storage subsystem may be displayed as individual end devices on the Fabric Manager map. To group end devices in a single enclosure in order to have them represented by a single icon on the map, follow these steps:

Step 1 Select **Storage** from the Fabric Manager's menu tree in the Physical tab.

The end devices are displayed in the Information pane.

Step 2 Clink on the **Name** field for one of the devices you want to be in the enclosure.

Step 3 Enter a name to identify the new enclosure's icon on the Fabric Manager Map pane.

Step 4 Enter the IP address of the device in the **IP Address** field (optional).

Step 5 Click once on the **Name** field for that device.

Step 6 Press Ctrl-C to copy that name.

Step 7 Clink on the **Name** field for another of the devices you want to be in the enclosure.

Click twice if there is no name in the Name field; click three times if there is a name already in the Name field.

Step 8 Press Ctrl-V to paste the name into the **Name** field for that device.

Step 9 Repeat steps 7 and 8 for each device you want to add to the enclosure.

Note To remove devices from an enclosure, triple click on the name of the device and press Delete. To remove an enclosure, repeat this step for each device in the enclosure. To change an existing enclosure, delete the enclosure and create a new one.

Creating a Policy Profile

You use a policy file to define the rules to be applied when running the Fabric Configuration Analysis tool. When you create a policy file, the system saves the rules selected for the selected switch.

To create a policy file, follow these steps:

Step 1 Choose **Tools** > **Fabric Configuration** from the Fabric Manager menu bar.

Step 2 Click **Policy File** and enter a name for the policy in the field provided.

Step 3 Click **Create Policy** and confirm the operation when prompted.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Setting Fabric Manager Preferences

To set your preferences for the behavior of the Fabric Manager, choose **File** > **Preferences** from the Fabric Manager menu bar. The Preferences dialog box is displayed.

This dialog box has the following tabs, which let you set your preferences for different components of the application:

- General
- Discovery
- Map

Viewing Reports in Fabric Manager

The Fabric Manager provides a series of reports, showing various information in tabular form. When you select one of these options, you see the available information in tabular form in the Information pane of the Fabric Manager main window. Table 3-2 describes the reports provided by each option.

Table 3-2 Fabric Manager Reports

Report	Description
ISL Statistics	Click on **Connectivity** > **ISLs** > **Statistics** in the Physical tab of the Fabric Manager Logical/Physical pane to display information about the Inter-Switch Links in the currently discovered fabric. You can use the controls at the top of the table to change the Poll Interval and Scale parameters:
ISLs	Choose **Connectivity** > **ISLs** in the Physical tab of the Fabric Manager Logical/Physical pane to display information about the Inter-Switch links in the currently discovered fabric.
Switches	Choose **Switches** in the Physical tab of the Fabric Manager Logical/Physical pane to display information about the switches in the currently discovered fabric.
Hosts	Choose **Connectivity** > **Hosts** in the Physical tab of the Fabric Manager Logical/Physical pane to display information about the hosts in the currently discovered fabric.
Storage	Choose **Connectivity** > **Storage** in the Physical tab of the Fabric Manager Logical/Physical pane to display information about the links to hosts and storage in the currently discovered fabric.
LUNs	Choose **Connectivity** > **Storage** > **LUNs** in the Physical tab of the Fabric Manager Logical/Physical pane to display information about the LUNs in the currently discovered fabric.

CHAPTER 4

Using Device Manager

Device Manager provides a physical representation of your switch chassis, with the modules, ports, power supplies, and fan assemblies (Figure 4-1). The menu bar at the top of the Device Manager window provides access to options, organized into menus that correspond to the menu tree in Fabric Manager.

The legend at the bottom right of the Device Manager indicates port status, as follows:

- Green—The port is up.
- Brown—The port is administratively down.
- Red—The port is down or has failed.
- Gray—The port is unreachable.

Launching Device Manager from Fabric Manager

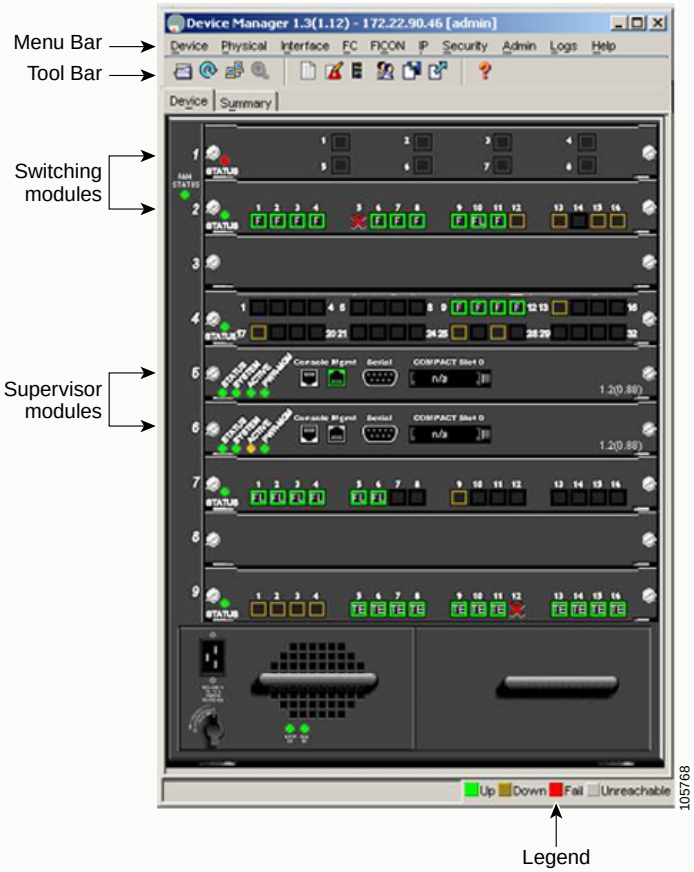
Device Manager gives a graphic representation of a Cisco MDS 9000 Family switch, including the installed switching modules, the supervisor modules, the power supplies, and the status of each port within each module.

To launch the Device Manager from your desktop, double-click the Device Manager icon and follow the instructions described in the "Launching the Applications" section on page 1-8.

To launch Device Manager from Fabric Manager, right-click the switch you want to manage on the Fabric Manager map and click **Device Manager** from the pop-up menu that appears. The Device Manager main window is shown in Figure 4-1.

Device Manager can also be started by double-clicking on a switch in the Fabric Manager topology view.

Figure 4-1 Device Manager, Device Tab



Using Summary View

Click the **Summary** tab on the Device Manager main window to see a summary of enabled interfaces on a single switch, as well as FC and IP neighbor devices. All logical interfaces are shown in a dropdown list at the top of the Summary view.

The Summary View displays attributes for a single switch, such as port speed, link utilization, and other traffic statistics. It has the same menu bar and toolbar buttons as the Device View.

To monitor traffic for selected objects, click the **Monitor** icon. To display detailed statistics for selected objects, click the **Detailed Statistics** icon.

The Summary View provides the same menus and options that are available from the Device View.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Device Manager help system.

Comparing Device Manager to Fabric Manager

The menu bar at the top of the Device Manager contains the same menus as the Fabric Manager menu tree.

For information about the options provided by these menus, see the "Logical/Physical Pane" section on page 3-4. The Device menu provides the following options:

- Open—Open the Device Manager for a different switch.
- Open Last—Open the Device Manager for the most recently managed switch.
- Preferences—Set management preferences for controlling the behavior and appearance of the Device Manager.
- Refresh—Update the current display.
- Command Line Interface—Open a Telnet/SSH session with the current switch.
- Exit—Close the Device Manager application.

The tables in the Fabric Manager roughly correspond to the dialog boxes that appear in Device Manager. However, the Fabric Manager tables show values for multiple switches and so the first column identifies the specific switch. The Device Manager dialog box shows values for a single switch, while the Fabric Manager shows the same values for one or more switches.

The toolbar on the Device Manager dialog box provides the same options as the toolbar on the Information pane in Fabric Manager, as summarized here:

- Create—Insert a new row into a table (if applicable).
- Delete Row—Delete the selected row from a table (if applicable).
- Copy…Ctrl+C — Copy data from one row to another.
- Paste…Ctrl +V—Paste the data from one row to another.
- Apply Changes—Apply configuration changes. (Note: After making changes you must save the configuration. Otherwise, the changes will be lost when the device is restarted.)
- Refresh Values—Refresh table values.
- Reset Changes…Ctrl-Z—Undo the most recent change.
- Print table…— Print the contents of the Information pane.

Tip You can copy values from one cell in a table to the rest of the column. Copy the value to the clipboard, hold down the shift key while pressing the down arrow key (or click on the bottom cell in the column). Then paste the value to all the selected cells and click **Apply**.

When you click the **Create** button, you see a dialog box that lets you enter the values required for the specific table. As you can see the fields and options are the same from both views, but the appearance of the window may vary slightly. For instance, the dialog box from Fabric Manager may have an option for selecting a specific switch, while the dialog box from Device Manager may have additional port-level detail.

Performing Device Management

Most tasks that you can perform with Device Manager can also be performed for multiple switches using the Fabric Manager. However, Device Manager may be more convenient to use when you are working with a single switch. Also, the Device Manager provides more detailed information for verifying or troubleshooting device-specific configuration than what is available from the Fabric Manager.

The Device View provides a graphic representation of a Cisco MDS 9000 switch, including the installed switching modules, services modules, supervisor modules, and the status of each port within each module. You can use the Device View to perform any switch-level configuration tasks including the following:

- Manage ports, Port Channels, and trunking
- Manage SNMPv3 security access to switches
- Manage CLI security access to switches
- Manage alarms, events, and notifications
- Save and copy configuration files and software images
- View hardware configuration
- View chassis, module, and port status and statistics

Summary View provides a way of monitoring all of the ports on the switch, categorized by operative modes (Fx-Ports and E-Ports).

When you click the Summary tab on the Device Manager window, you see the Summary View, which provides summary information about the interfaces on a single switch.

Managing Ports

Tip You can select multiple ports in Device Manager and apply options to all the selected ports at one time. Either select the ports by clicking the mouse and dragging it around them, or hold down the Control key and click on each port.

To enable or disable a port, right-click the port and click **Enable** or **Disable** from the pop-up menu. To enable or disable multiple ports, drag the mouse to select the ports and then right-click the selected ports. Then click **Enable** or **Disable** from the pop-up menu.

To manage trunking on one or more ports, right-click the ports and click **Configure**. On the dialog box that appears, in the Trunk column, right-click the current value and click **nonTrunk**, **trunk**, or **auto** from the pull-down list.

To create PortChannels using Device Manager, click **PortChannels** from the Interface menu. For detailed instructions, see the "Managing PortChannel Interfaces" section on page 8-4. You can also use Fabric Manager to conveniently create a PortChannel.

Note To create a PortChannel, all the ports on both ends of the link must have the same port speed, trunking type, and administrative state.

Setting Device Manager Preferences

To set your preferences for the behavior of the Device Manager application, choose **Preferences** from the Device menu.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Device Manager help system.

CHAPTER 5

Using Performance Manager

Performance Manager monitors network device statistics historically, and provide this information graphically using a web browser. It presents recent statistics in detail and older statistics in summary. Performance Manager also integrates with external tools, such as Cisco Traffic Analyzer.

Performance Manager Architecture

The Performance Manager has three parts:

- Definition - use a configuration wizard to create a configuration file
- Collection - Performance Manager reads the configuration file and collects the desired information
- Presentation - Performance Manager generates web pages to present the collected data

Performance Manager can collect a variety of data, about these fabric components: ISLs, host ports, storage ports, route flows, and site-specific statistical collection areas.

Creating a PM Configuration File

Performance Manager has a Configuration File Wizard, which steps you through the process of creating configuration files.

Step 1 Launch the wizard by selecting Create Collection from the Performance menu in Fabric Manager.

Step 2 Select the VSANs from which you want to collect data.

Step 3 Check the types of SAN objects for which you want to collect data.

Step 4 If you want to ignore flows with Zero counter values, check that checkbox.

Step 5 If you are using Cisco Traffic Analyzer, enter the URL where it is located on your network.

Step 6 Click Next to review the collected data.

Step 7 Enter the name of the file (the default is the switch's IP address with a .XML suffix).

Step 8 Select the definitions that you wish to remove, then click Finish to create the configuration file.

Collecting the Data

One year's worth of data for two variables (Rx and Tx Bytes) requires an rrd file size of 76K. The default internal values are:

- 600 samples of 5 minutes (2 days and 2 hours)

- 700 samples of 30 minutes (2 days and 2 hours, plus 12.5 days)
- 775 samples of 2 hours (above + 50 days)
- 300 samples of 1 day (above + 300 days, rounded up to 365)

A 1000-port SAN requires 76MB for a year's worth of historical data. If there were 20 switches in this SAN with equal distribution of fabric ports, about 2-3 SNMP packets per switch would be sent every 5 minutes for a total of about 100 total request/response SNMP packets required to monitor the data.

Flows, because of their variable counter requests, are more difficult to predict. But as a rule of thumb, each extra variable adds another 38K.

The Performance Manager collector is designed to run as a background process on the various supported OSs. On MS Windows, it runs as a service.

Presenting the Collected Data

The Summary page presents the top 10 Hosts, ISLs, Storage, and Flows by average throughput for the last 24 hour period. This period changes on every polling interval – this is unlikely to change the average significantly, but it could affect the maximum value. The intention is to provide a quick summary of the fabric's bandwidth consumption and highlight any hotspots.

- Clicking on any Host, Storage, ISL, or Flow title will provide a view of traffic over the past day for all Hosts, Storage, ISLs, or Flows respectively.
- Clicking on a host port from the summary page will provide you with a similar detail page. If flows exist for that port, you could see which storage ports it was sending data to.
- Clicking on the ISLs link from the summary page will list the daily traffic charts for all monitored ISLs in the fabric.

Exporting and Importing Data

You can export an rrd file to XML with the command:

pm xport <rrdFile> <xmlFile>

This will produce an XML format that rrdtool is capable of reading with the command:

rrdtool restore *filename.xml filename.rrd.*

You can import an XML with the command:

pm restore <xmlFile> <rrdFile>

This will read the XML export format that *rrdtool* is capable of writing with the command:

rrdtool xport *filename.xml filename.rrd.*

Integration with Cisco Traffic Analyzer

SNMP and Performance Manager can only provide a top-level view of what data the fabric is carrying. The Cisco MDS 9000 switch has no LUN-level flow counters, and cannot count SCSI commands. In order to view this detailed information, it is necessary to look at the data on a SPAN destination port with the help of the Cisco Traffic Analyzer, which uses the Cisco Port Adapter Analyzer.

Cisco Traffic Analyzer must be downloaded and installed separately.

Caution The Cisco Traffic Analyzer for Fibre Channel throughput values are not accurate when used with the original Cisco Port Adapter Analyzer if data truncation is enabled. The A version of the Cisco Port Adapter Analyzer is required to achieve accurate results with truncation, because it adds a count that enables the Cisco Traffic Analyzer to determine how many data bytes were actually transferred.

CHAPTER 6

Managing the System and Components

The Fabric Manager allows you to configure and monitor modules on multiple Cisco MDS 9000 switches. The Device Manager allows you to configure and monitor modules on a single Cisco MDS 9000 switch.

Note For information about configuring the chassis and its components using the command-line interface (CLI), refer to the *Cisco 9000 Family Configuration Guide*.

Procedures for managing the system and components include:

Viewing System Attributes

To manage system attributes, perform the following steps.

Step 1 From the Fabric Manager, choose **Switches** on the menu tree, OR
From the Device Manager, choose **System** from the Admin menu. (You can also double click on the chassis in Device Manager.)

The Fabric Manager Information pane displays system attributes for multiple switches. The dialog box from the Device Manager displays system attributes for a single switch.

Step 2 Configure the system attributes for the chassis.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Viewing Running Processes

To view information about the processes currently running on a switch, perform the following step.

Step 1 From the Device Manager, choose **Running Processes** from the Admin menu.

You see the Running Processes dialog box.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Viewing Flash File Information

To view information about the files currently stored in flash memory on the switch, perform the following step.

Step 1 From the Device Manager, choose **Flash Files** from the Admin menu.

You see the Flash Files dialog box.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Managing Inventory Information

To manage inventory attributes, perform the following steps.

Step 1 From the Fabric Manager, choose **Switches** > **Modules** on the menu tree and click the **Inventory** tab, OR From the Device Manager, choose **Inventory** from the **Physical** menu.

The Fabric Manager Information pane displays system attributes for multiple switches. The dialog box from the Device Manager displays system attributes for a single switch.

Step 2 Configure the inventory attributes for the module.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Managing Card Attributes

To manage card status attributes, perform the following steps.

Step 1 From the Fabric Manager, choose **Switches** > **Modules** on the menu tree and click the **Card Status** tab, OR
From the Device Manager, choose **Modules** from the Physical menu.

The Information pane from the Fabric Manager displays card attributes for multiple switches. The dialog box from the Device Manager view displays attributes for a single switch.

Step 2 Configure the status attributes for the module.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Managing Temperature Sensor Information

To monitor sensor temperature attributes, perform the following steps.

Step 1 From the Fabric Manager, choose **Switches > Modules** on the menu tree and click the **Temperature Sensors** tab, OR
From the Device Manager, choose Temperature **Sensors** from the **Physical** menu.

The Information pane from the Fabric Manager displays sensor temperature attributes for multiple switches. The Sensors dialog box from the Device Manager displays sensor temperature attributes for a single switch.

Step 2 Configure the sensor attributes.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Managing Power Supplies

To manage power supply power attributes, perform the following steps.

Step 1 From the Fabric Manager, choose **Switches** > **Modules** on the menu tree and click the **Power Supplies** tab, OR
From the Device Manager, choose **Power Supplies** from the Physical menu.

The Information pane from the Fabric Manager displays power supply power attributes for multiple switches. The dialog box from the Device Manager displays power supply power attributes for a single switch.

Step 2 Configure the power attributes for the power supply.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Managing Network Time Protocol (NTP)

You can create or view NTP peers and servers from the Fabric Manager or Device Manager. You do not need to specifically enable NTP on a peer or server. If there is an entry, then "enabled" is implied.

The list below shows the NTP tasks you can perform.

- Display General NTP Statistics for a Switch, page 6-4
- Create an NTP Server or Peer, page 6-4
- Edit an NTP Server or Peer Configuration, page 6-5
- Delete an NTP Server or Peer, page 6-6

Display General NTP Statistics for a Switch

To display general NTP statistics for a switch, perform the following steps.

Step 1 From the Fabric Manager, select **Switches > System** from the Physical pane of the menu tree, OR
From Device Manager, choose **NTP** from the **Admin** menu.

The System information pane (or in DM, the NTP dialog box) is displayed.

Step 2 Click the **NTP General** tab.

The general NTP statistics for that switch are displayed.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Create an NTP Server or Peer

To create an NTP server or peer, perform the following steps.

Step 1 From the Fabric Manager, select **Switches > System** from the Physical pane of the menu tree, OR From Device Manager, choose **NTP** from the **Admin** menu.

The System information pane (or in DM, the NTP dialog box) is displayed.

Step 2 Click the **NTP Peer** tab.

A list of NTP peers and servers for that switch is displayed.

Step 3 Click the **Create** button.

The Create NTP Peer dialog box is displayed.

Step 4 Enter the peer address in the Peer Address field.

Step 5 Select the mode (peer or server).

Step 6 Click the PrefPeer checkbox if you want this peer to be a Preferred Peer.

Step 7 Click the **Create** button to create the peer or server; click the **Close** button to close the Create NTP Peer dialog box without creating the peer or server.

The newly created peer or server is listed under the Peer tab.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Edit an NTP Server or Peer Configuration

To create an NTP server or peer, perform the following steps.

Step 1 From the Fabric Manager, select **Switches > System** from the Physical pane of the menu tree, OR From Device Manager, choose **NTP** from the **Admin** menu.

The System information pane (or in DM, the NTP dialog box) is displayed.

Step 2 Click the **NTP Peer** tab.

A list of NTP peers and servers for that switch is displayed.

Step 3 To change the peer address, double click on the IP address in the Peer Address column, and change the numbers. Alternatively, you can triple click on the IP address and type in a new address.

Step 4 To change the mode from peer to server, click on the mode in the Mode column next to the address of the switch for which you want to change the mode.

A dropdown list is displayed with the options **peer** or **server**. Select the mode you want for your switch.

Step 5 To change the Preferred Peer status to Preferred Peer, check the **PrefPeer** checkbox next to the address of the switch for which you want to change the status. To remove this status, uncheck the box.

Step 6 Click the **Apply** button to apply your changes to the switch, or click the **Close** button to close the NTP Peer dialog box without saving your changes.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Delete an NTP Server or Peer

To delete an NTP server or peer, perform the following steps.

Step 1 From the Fabric Manager, select **Switches > System** from the Physical pane of the menu tree, OR From Device Manager, choose **NTP** from the **Admin** menu.

The System information pane (or in DM, the NTP dialog box) is displayed.

Step 2 Click the **NTP Peer** tab.

A list of NTP peers and servers for that switch is displayed.

Step 3 To delete a server or peer, click on the IP address in the Peer Address column.

Step 4 The Delete button is enabled.

Step 5 Click the **Delete** button to delete the peer or server, or click the **Close** button to close the NTP Peer dialog box without deleting the peer.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Managing Events and Alarms

By configuring how events are reported, you can monitor those events more effectively and take corrective action, if necessary. Cisco Fabric Manager provides the following features for reporting and responding to network events.

SNMP events

These are preconfigured notifications, including SNMPv2 traps and SNMPv3 informs. Procedures for managing SNMP events include:

- Viewing the Events Log, page 6-8
- Configuring Event Destinations, page 6-8
- Configuring Event Security, page 6-9
- Configuring Event Filters, page 6-9

RMON alarms

These are configurable notifications that you can set based on thresholds for various network events. Procedures for managing and viewing RMON alarms include:

- Enabling RMON Alarms by Port, page 6-9
- Enabling RMON Alarms for VSANs, page 6-10
- Enabling RMON Alarms for Physical Components, page 6-10
- Configuring RMON Controls, page 6-11
- Managing RMON Alarms, page 6-11
- Managing RMON Event Severity Levels, page 6-11
- Viewing the RMON Log, page 6-12

Call Home

This is a feature that lets you configure automatically generated e-mail messages or other responses to specific events. You can use Call Home for direct paging of a network support engineer, E-mail notification to a Network Operations Center, and utilization of Cisco AutoNotify services for direct case generation with the Cisco Technical Assistance Center. Call Home provides the following features:

- Fixed set of predefined alerts and trigger events on the switch.
- Automatic execution and attachment of relevant command output.
- Multiple message format options:
  - Short Text — Suitable for pagers or printed reports.
  - Plain Text — Full formatted message information suitable for human reading.
  - XML — Matching readable format using Extensible Markup Language (XML) and Document Type Definitions (DTDs) named Messaging Markup Language (MML). The MML DTD is published on the Cisco Connection Online (CCO) website at http://www.cisco.com/. The XML format enables communication with the Cisco Systems TAC group.
- Multiple concurrent message destinations. Up to 50 e-mail destination addresses are allowed for each format type.
- Message categories include system, environment, switching module hardware, services module hardware, supervisor module, hardware, inventory, and test.

Procedures for configuring Call Home include:

- Call Home Configuration Overview, page 6-12
- Configuring Call Home Attributes, page 6-13
- Configuring Call Home Destination Attributes, page 6-13
- Configuring Call Home E-Mail Addresses, page 6-14
- Configuring Call Home Alerts, page 6-14
- Configuring Call Home Profiles, page 6-14

Syslog

This is a standard message log that records various network and system events. Procedures for configuring the Syslog include:

- Configuring Syslog Attributes, page 6-15
- Configuring Syslog Servers, page 6-15
- Configuring Syslog Priorities, page 6-16

Note The Fabric Manager allows you to manage events on multiple Cisco MDS 9000 Family switches. The Device Manager allows you to manage events on a single Cisco MDS 9000 Family switch.

For information about events and configuring them using the command-line interface (CLI), refer to the *Cisco 9000 Family Configuration Guide*.

Viewing the Events Log

To view the events log from the Device Manager, choose **SNMP Log** from the Events menu. The Events Log dialog box displays a log of events for a single switch

To manage the SNMP log, choose **SNMP Log** from the Events menu and click the **Controls** tab. The Controls tab provides summary statistics about the SNMP log and allows you to change the default settings for the log.

Caution Changing these values from different Fabric Manager workstations at the same time may cause unpredictable results.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Configuring Event Destinations

Cisco MDS 9000 Family switches, like other SNMP-enabled devices, send events (traps and informs) to configurable destinations, called trap receivers in SNMPv2.

To configure event destinations from the Fabric Manager, choose **Events > Notifications/Traps** on the menu tree and click the **Destinations** tab. To configure event destinations from the Device Manager, choose **Destinations** from the Events menu.

The Information pane from the Fabric Manager displays event destination information for multiple switches. The dialog box for the Device Manager displays event destinations for a single switch.

To create an event destination, click **Create** on the Device Manager dialog box or click the **Create Row** button on the Fabric Manager toolbar.

The Create Event Destinations dialog box is displayed. The dialog box from the Fabric Manager lets you select a switch.

Complete the fields and click **Apply** to create the event destination or click **OK** to create the destination and close the window.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Configuring Event Security

Caution This is an advanced function that should only be used by administrators having experience with SNMPv3.

To configure event security from the Fabric Manager, choose **Events > Notifications/Traps** on the menu tree, and click the **Security** tab.

To configure event security from the Device Manager, choose **Destinations** from the Events menu and click the **Security** tab.

The Information pane from the Fabric Manager displays event security information for multiple switches. The dialog box from Device Manager displays event security for a single switch.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Configuring Event Filters

To configure event filters from the Fabric Manager, choose **Events** > **Filters** on the menu tree, and click the **FC** or **Other** tab.

To configure event filters from the Device Manager, choose **Filters** from the Events menu.

The Event Filters dialog box displays event filters for a single switch. The Information pane in Fabric Manager displays two different views, which list the same event filters for multiple switches, in different order.

To configure event filters, check the check box next to the appropriate filter name.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Enabling RMON Alarms by Port

To enable alarm notifications by port from the Device Manager, choose **Threshold Manager** from the **Events** menu and click the **Ports** tab.

To configure an RMON alarm for one or more ports, follow these steps:

Step 1 Click the **Selected** radio button.

Step 2 Click the button to the right of the Selected field to display all ports.

Step 3 Select the ports you want to monitor.

Step 4 Click OK to accept the selection.

Alternatively, click the appropriate radio button to select ports by type - All ports, xE ports, or Fx ports

Step 1 Click the check box for each variable that you want to monitor.

Step 2 Enter the threshold value in the Value column.

Step 3 Enter the sampling period in seconds.

Step 4 Select one of the following severity levels to assign to the alarm - Fatal, Warning, Critical, Error, Information

Step 5 Click **Create**.

Step 6 Confirm the operation to define an alarm and a log event when the system prompts you to define a severity event.

If you do not confirm the operation, the system only defines a log event.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Enabling RMON Alarms for VSANs

To manage RMON alarm service attributes for selected VSANs from the Device Manager, choose **Threshold Manager** from the Events menu and click the **Services** tab. The Threshold Manager dialog box with the Services tab selected is displayed.

To enable an RMON alarm for one or more VSANs, follow these steps:

Step 1 Enter one or more VSANs to monitor in the VSAN Id(s) field.

Step 2 Click the check box for each variable that you want to monitor.

Step 3 Enter the threshold value in the Value column.

Step 4 Enter the sampling period in seconds.

Step 5 Select a severity level to assign to the alarm:

Step 6 Click **Create**.

Step 7 Confirm the operation to define an alarm and a log event when the system prompts you to define a severity event.

If you do not confirm the operation, the system only defines a log event.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Enabling RMON Alarms for Physical Components

To configure RMON alarm physical attributes from the Device Manager, choose **Threshold Manager** from the Events menu and click the **Physical** tab. The **Create RMON Alarms** dialog box with the Physical tab selected is displayed.

To configure an RMON alarm for a physical component, follow these steps:

Step 1 Click the check box for each variable that you want to monitor.

Step 2 Enter the threshold value in the Value column.

Step 3 Enter the sampling period in seconds.

Step 4 Select one of the following severity levels to assign to the alarm:

- Fatal
- Warning
- Critical
- Error
- Information

Step 5 Click **Create**.

Step 6 Confirm the operation to define an alarm and a log event when the system prompts you to define a severity event.

If you do not confirm the operation, the system only defines a log event.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Configuring RMON Controls

To change the default controls for RMON alarms, choose **Threshold Manager** from the Device Manager menu. You see the Threshold Manager window.

Click **More** on the Threshold Manager window. You see the second Threshold Manager dialog box.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Managing RMON Alarms

To view the alarms that have already been enabled, do the following:

Step 1 Choose **Threshold Manager** from the Events menu and click the **More** button on the Threshold Manager dialog box.

Step 2 Click the **Alarms** tab.

You see the RMON Alarms dialog box.

Step 3 To create a customized threshold entry, click the **Create** button.

You see the Create RMON Alarms dialog box.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Managing RMON Event Severity Levels

To define customized RMON event severity levels, do the following:

Step 1 Select **Threshold Manager** from the Events menu and click **More** on the Threshold Manager dialog box.

Step 2 Click the **Events** tab on the RMON Thresholds dialog box.

You see the RMON Events dialog box.

Step 3 To create a new threshold entry, click the **Create** button.

You see the Create Threshold Entry dialog box.

Step 4 Configure the RMON event threshold attributes.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Viewing the RMON Log

To view the RMON log from the Device Manager, do the following:

Step 1 Select **Threshold Manager** from the Events menu and click **More** on the Threshold Manager dialog box.

Step 2 Click the **Log** tab on the RMON Thresholds dialog box.

You see the RMON Log dialog box.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Call Home Configuration Overview

When configuring Call Home, keep the following points in mind:

- You must configure at least one E-mail server and at least one destination profile. The destination profile(s) used depends on whether the notification is sent to a pager, e-mail, or automated service such as Cisco AutoNotify.
- You must configure the contact name (SNMP server contact), phone, and street address information before enabling Call Home.
- The Cisco MDS 9000 switch must have IP connectivity to an E-mail server.
- To use Cisco AutoNotify you must obtain an active service contract for the device.

To configure Call Home, use the different tabs on the Call Home dialog box, as summarized below:

Step 1 Assign contact information and enable the Call Home feature using the General tab (see the "Configuring Call Home Attributes" section on page 6-13). The Call Home feature is not enabled by default, and you must enter an e-mail address that identifies the source of Call Home notifications.

Step 2 Configure the destination e-mail addresses for Call Home notifications using the Destinations tab (see the "Configuring Call Home Destination Attributes" section on page 6-13). You can identify one more more e-mail addresses that will receive Call Home notifications.

Step 3 Identify your SMTP server using the E-mail Setup tab (see the "Configuring Call Home E-Mail Addresses" section on page 6-14). You need to identify a message server to which your switch has access. This message server will forward the Call Home notifications to the destinations.

Step 4 Test Call Home by sending a test message using the Alerts tab (see the "Configuring Call Home Alerts" section on page 6-14). You should test the Call Home feature to make sure it works.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Configuring Call Home Attributes

To assign contact information and enable the Call Home feature from the Fabric Manager, choose **Events** > **Call Home** on the menu tree and click the **General** tab. The Information pane from the Fabric Manager displays Call Home information for multiple switches.

To assign contact information and enable the Call Home feature from the Device Manager, choose **Call Home** from the Events menu and click the **General** tab. The Call Home Events dialog box with the General tab selected from the Device Manager displays Call Home attributes for a single switch.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Configuring Call Home Destination Attributes

To configure the destination e-mail addresses for Call Home notifications from the Fabric Manager, choose **Events** > **Call Home** on the menu tree and click the **Destination** tab. The Information pane from the Fabric Manager displays Call Home information for multiple switches.

To configure the destination e-mail addresses from the Device Manager, choose **Call Home** from the Events menu and click the **Destination** tab. The dialog box from the Device Manager displays Call Home attributes for a single switch.

To create a new Call Home destination, follow these steps:

Step 1 Click **Create** on the Device Manager dialog box, or click the **Create Row** button on the Fabric Manager toolbar.

From the Device Manager, you see the Create Call Home Destination dialog box.

From the Fabric Manager, you can select one or more switches to which the configuration applies.

Step 2 Select the profile name from the pull-down list.

Step 3 Enter a number identifier for the destination.

Step 4 Enter the e-mail address for the destination.

Step 5 Click **Create**.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Configuring Call Home E-Mail Addresses

To identify your SMTP server from the Fabric Manager, choose **Events** > **Call Home** on the menu tree and click the **Email Setup** tab. The Information pane from the Fabric Manager displays Call Home information for multiple switches.

To identify your SMTP server from the Device Manager, choose **Call Home** from the Events menu and click the **Email Setup** tab. The Call Home dialog box from the Device Manager displays Call Home attributes for a single switch.

Configure the e-mail setup attributes for the Call Home features.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Configuring Call Home Alerts

To test Call Home from the Fabric Manager, choose **Events** > **Call Home** the menu tree and click the **Alerts** tab. The Information pane from the Fabric Manager displays Call Home information for multiple switches.

To test Call Home from the Device Manager, choose **Call Home** from the Events menu and click the **Alerts** tab. The dialog box with the Alerts tab selected from the Device Manager displays Call Home attributes for a single switch.

Configure the alert attributes for the Call Home feature.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Configuring Call Home Profiles

To configure Call Home attributes from the Fabric Manager, choose **Events** > **Call Home** on the menu tree and click the **Profiles** tab. The Information pane from the Fabric Manager displays Call Home information for multiple switches.

To configure Call Home attributes from the Device Manager, choose **Call Home** from the Events menu and click the **Profiles** tab. The dialog box with the Alerts tab selected from the Device Manager displays Call Home attributes for a single switch.

Configure the profile attributes for the Call Home feature.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Configuring Syslog Attributes

To configure syslog attributes, do the following:

Step 1 From the Fabric Manager, choose **Events** > **Syslog** on the menu tree and click the **General** tab. The Information pane from the Fabric Manager displays syslog information for multiple switches.

From the Device Manager, choose **Syslog** from the Events menu and click the **General** tab. The Syslog dialog box with the General tab selected from the Device Manager displays syslog information for a single switch.

Step 2 Configure the general attributes for the syslog.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Configuring Syslog Servers

To configure syslog servers, do the following:

Step 1 From the Fabric Manager, choose **Events** > **Syslog** on the menu tree and click the **Servers** tab. The Information pane from the Fabric Manager displays syslog information for multiple switches.

From the Device Manager, choose **Syslog** from the Events menu and click the **Servers** tab. The Syslog dialog box with the Servers tab selected from the Device Manager displays syslog information for a single switch.

Step 2 Configure the server attributes for the syslog.

Step 3 To add a syslog server, click **Create**.

You see the Create Syslog Server dialog box.

Step 4 Complete the fields on this dialog box and click **OK**.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Configuring Syslog Priorities

To configure syslog priorities, do the following:

Step 1 From the Fabric Manager, choose **Events > Syslog** on the menu tree and click the **Priorities** tab. The Information pane from the Fabric Manager displays syslog information for multiple switches.

From the Device Manager, choose **Syslog** from the Events menu and click the **Priorities** tab. To configure syslog attributes The Syslog dialog box with the Servers tab selected from the Device Manager displays syslog information for a single switch.

Step 2 Configure the priorities for the syslog.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Managing Software and Configuration Files

Note For more information about managing software image and configuration files using the command-line interface (CLI), refer to the *Cisco 9000 Family Configuration Guide* or the *Cisco 9000 Family Command Reference*.

Each switch in the Cisco MDS 9000 Family is shipped with a Cisco Multilayer intelligent SAN operating system called SAN-OS, and two images:

- The kickstart image—Loads the kernel and basic drivers
- The system image—Loads the system image

To upgrade to a different software version, you need to download the new image software to your local switch. To start running the new image files, use the CLI to change the relevant configuration variables to point to the new images and restart the switch.

All Cisco MDS 9000 Family switches contain internal bootflash memory that resides in the supervisor module. Cisco MDS 9500 Series directors contain an additional external CompactFlash called slot0.

Upgrading a software image does not disrupt use of the startup configuration file, which you can still use after the upgrade. When you restart the switch, the startup configuration is converted so that it is usable by the new image.

CHAPTER 7

Managing VSANs

VSANs (virtual SANs) allow you to isolate devices that are physically connected to the same fabric, and thus provide higher security and greater scalability in the network fabric. When you create VSANs, you are creating multiple logical SANs over a common physical infrastructure. After creating VSANs, you must establish IP static routes between the network segments if you are using the IP over Fibre Channel (IPFC) protocol to manage your Cisco MDS 9000 Family switches.

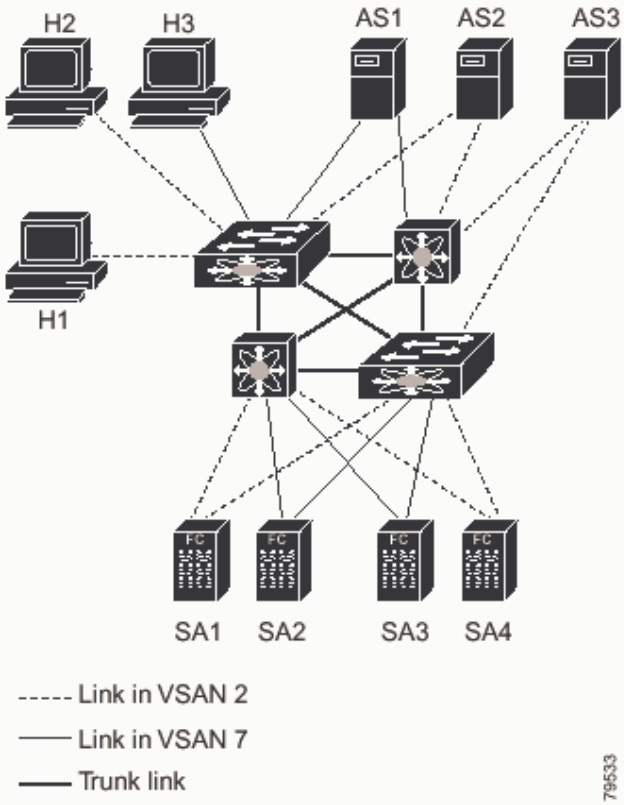
The Fabric Manager allows you to configure VSANs on multiple Cisco MDS 9000 switches. The Device Manager allows you to configure VSANs on a single Cisco MDS 9000 switch.

Note For information about VSANs and configuring them using the command-line interface (CLI), refer to the *Cisco 9000 Family Configuration Guide.*

You can manage Cisco MDS 9000 Family switches through Ethernet connections to the management interface (mgmt 0) of each switch or by using the IPFC protocol. To use IPFC, you connect to a switch using the Ethernet management interface and establish routes from that switch to the other switches over the Fibre Channel network. When you segment the Fibre Channel network using VSANs, you must establish static routes between the network segments.

Figure 7-1 shows a physical Fibre Channel network with two VSANs. VSAN 2 is connected by dashed lines and VSAN 7 is connected by solid lines.

Figure 7-1 Configuring VSANs



VSAN 2 includes the H1 and H2 hosts, the AS2 and AS3 application servers, and the SA1 and SA4 storage arrays. VSAN 7 connects H3, AS1, SA2, and SA3. The four switches in this network are interconnected by trunk links that carry both VSAN 2 and VSAN 7 traffic.

VSAN 1 is the default VSAN for Cisco MDS 9000 Family switches. All ports are assigned by default to VSAN 1. VSAN 4094 is called the isolated VSAN. When a VSAN is deleted, any ports in that VSAN are moved to VSAN 4094.

Note We recommend that you delete or move all the ports in a VSAN before deleting the VSAN.

VSANs are enabled through trunking, which enables interconnect ports to transmit and receive frames in more than one VSAN over a single physical link, using the Extended Inter-Switch Link (EISL) protocol. The trunking protocol is enabled by default, and if disabled on a switch, no ports on that switch or directly connected to the switch will support the use of VSANs.

By default, the trunk mode is enabled on all Fibre Channel interfaces, but can be disabled on a port-by-port basis. When connected to a third-party switch, the trunk mode configuration has no effect—the ISL is always in a trunking disabled state.

Each Fibre Channel interface has an associated trunk-allowed VSAN list. This list determines the VSANs that are supported on each interface. By default, the entire range of VSANs from 1 through 4093 are allowed on any interface. You can restrict an interface to the use of a specific set of VSANs, which prevents traffic from any other VSAN being transmitted on the interface.

Procedures for managing VSANs include:

- Adding and Configuring VSANs, page 7-3

Adding and Configuring VSANs

To add and configure VSANs, perform the following steps.

Step 1 From the Fabric Manager, click on the desired VSAN from the menu tree in the Logical pane, OR From Device Manager, choose the **VSAN** option from the FC menu or click the **VSAN** icon on the toolbar.

The Fabric Manager's Information pane displays VSAN attributes for multiple switches. The VSAN dialog box in the Device Manager displays VSAN general attributes for a single switch.

Step 2 From Fabric Manager, click the **Create VSAN** button on the Information pane toolbar, OR From Device Manager, click **Create** on the VSAN dialog box.

You see the Create dialog box.

Step 3 Complete the fields on this dialog box and click **Create** to add the VSAN.

Controlling In-Band Management Connectivity

The Fabric Manager allows you to configure and monitor IP traffic on multiple Cisco MDS 9000 Family switches. The Device Manager allows you to configure and monitor IP traffic on a single Cisco 9000 switch.

Cisco MDS 9000 Family switches support both out-of-band and in-band management schemes. An Ethernet connection provides out-of-band management using Telnet, SSH or SNMP access. In-band IP management is also available using IP over Fibre Channel (IPFC). IPFC encapsulates IP packets into Fibre Channel frames so that management information can cross the Fibre Channel network without requiring a dedicated Ethernet connection to each switch. IP addresses are resolved to the Fibre Channel address through the Address Resolution Protocol (ARP).

Procedures for managing and viewing connectivity information include:

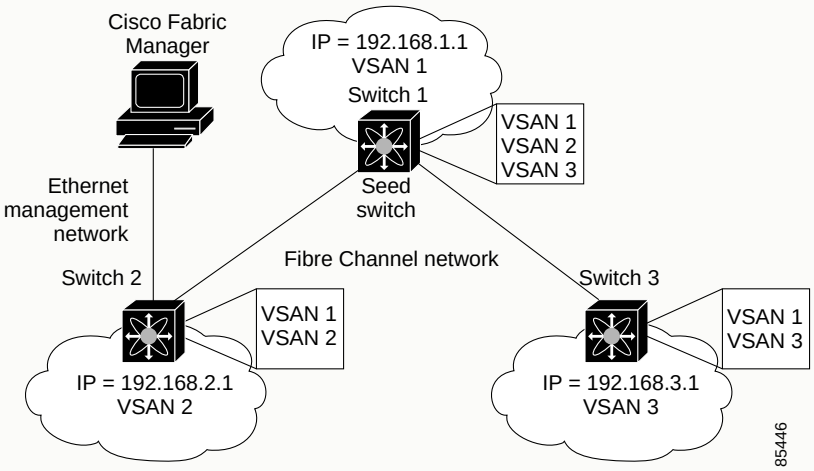
- Configuring IP Routing for Management Traffic, page 7-4
- Managing IPFC Connectivity with Multiple VSANs, page 7-5
- Viewing IP Address Information, page 7-5
- Enabling or Disabling IP Forwarding, page 7-5
- Viewing TCP Information and Statistics, page 7-6
- Viewing UDP Information and Statistics, page 7-6
- Viewing IP Statistics, page 7-6
- Viewing ICMP Statistics, page 7-6

- Monitoring SNMP Traffic, page 7-7

Configuring IP Routing for Management Traffic

When using in-band network management over Fibre Channel links, you must ensure that a path exists from the seed switch, connected to the Cisco Fabric Manager over its Ethernet interface (mgmt0), and the other switches in the network fabric. See Figure 7-2.

Figure 7-2 IP Routing Between VSANs



To do this, make sure that the seed switch has a path to each VSAN. Each of the other switches can then be configured to use the seed switch as their default gateway. For example, in Figure 7-2, switch 1 is connected to VSAN 2 and VSAN 3, while switch 2 and switch 3 are configured to use switch 1 as their default gateway.

You can also configure static routes on a point-to-point basis from one switch to another. In this example, you would configure a static route on both switch 2 and switch 3 to switch 1.

Configuring an IP Route

To configure an IP route or identify the default gateway, perform the following steps.

Step 1 From the Device Manager, choose **Routes** from the **IP** menu.

You see the IP Routes window.

Step 2 To create a new IP route or identify the default gateway on a switch, click the **Create** button.

You see the Create IP Routes window.

Step 3 Complete the fields on this window and click **OK** to add an IP route.

Step 4 To configure a static route, enter the destination network ID and subnet mask in the Dest and Mask fields. To configure a default gateway, enter the IP address of the seed switch in the Gateway field.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Managing IPFC Connectivity with Multiple VSANs

To configure IPFC from the Device Manager, choose **VSAN** from the FC menu and click the **General** tab.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Viewing IP Address Information

To view IP addresses of the switches in the current fabric from the Fabric Manager, choose **Switches** from the menu tree.

The Information pane displays IP address information for multiple switches.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Enabling or Disabling IP Forwarding

To view or change the IP forwarding configuration of the switches in the current fabric, perform the following steps.

Step 1 Choose **IP** > **Forwarding** from the Fabric Manager menu tree.

Step 2 To enable IP forwarding for a specific switch, click the **RoutingEnabled** check box.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Viewing TCP Information and Statistics

To view TCP information from the Device Manager, choose **Mgmt TCP/UDP** from the IP menu.

To monitor TCP statistics from the Fabric Manager, choose **IP > Mgmt Statistics** from the menu tree and click the **TCP** tab. To monitor TCP statistics from the Device Manager, choose **Statistics** from the IP menu and view the TCP tab.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Viewing UDP Information and Statistics

To view User Datagram Protocol (UDP) information, from the Device Manager, choose **Mgmt TCP/UDP** from the IP menu and click the **UDP** tab.

To monitor UDP traffic from the Fabric Manager, choose **IP > Mgmt Statistics** from the menu tree and click the **UDP** tab. From Device Manager, choose **Statistics** from the IP menu and click the **UDP** tab.

The Fabric Manager Information pane displays TCP traffic information for multiple switches. The Device Manager dialog box displays information for a single switch.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Viewing IP Statistics

To monitor IP statistics from the Fabric Manager, choose **IP** >**Mgmt Statistics** from the menu tree and click the **IP** tab. From Device Manager, select **Statistics** from the IP menu and click the **IP** tab.

The Fabric Manager Information pane displays IP statistics for multiple switches. The Device Manager dialog box displays information for a single switch.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Viewing ICMP Statistics

To monitor statistics for ICMP packets received, select **IP** > **Mgmt Statistics** from the menu tree and click the **ICMP In** tab. To monitor statistics for ICMP packets transmitted from the Fabric Manager, select **IP** > **Mgmt Statistics** from the menu tree and click the **ICMP Out** tab.

To monitor ICMP statistics from Device Manager, select **Statistics** from the IP menu and click the **ICMP** tab.

The Fabric Manager Information pane displays information for multiple switches. The Device Manager dialog box displays information for a single switch.

In the Device Manager, a prefix (In or Out) identifies whether the packets are received or transmitted. In the Fabric Manager, separate tabs on the Information pane are provided for incoming and outbound ICMP traffic and this prefix is omitted.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Monitoring SNMP Traffic

To monitor SNMP traffic statistics from the Fabric Manager, select **IP** >**Mgmt Statistics** from the menu tree and click on the **SNMP** tab. To monitor SNMP traffic from Device Manager, select **Statistics** from the IP menu and click the **SNMP** tab.

The Fabric Manager Information pane displays information for multiple switches. The Device Manager dialog box displays information for a single switch.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

CHAPTER 8

Managing Interfaces

Fabric Manager allows you to configure and monitor interfaces on multiple Cisco 9000 switches. The Device Manager allows you to configure and monitor interfaces on a single Cisco 9000 switch.

For information about interfaces and configuring them using the command-line interface (CLI), refer to the *Cisco 9000 Family Configuration Guide.*

Procedures for managing interfaces fall under three general categories:

Managing General Port Attributes

To manage general port attributes, such as Alias, PortVsan, and Admin Mode from the Fabric Manager, select the **Physical** tab at the bottom of the screen and choose **IP** or **FC** from the menu tree.

To manage these attributes from the Device Manager, select a port, and then choose that type of port from the Interface menu. You can select FxPorts, xEPorts, Enabled Ports, All Ports, or the Mgmt Port.

The following are the different port types supported by the Cisco MDS 9000 Family.

- xE ports:
  - An E_Port (expansion port) connects two switches and can carry frames between switches for configuration and management of the fabric for a single VSAN.
  - A TE_Port (trunking expansion port) allows a link between two Cisco 9000 switches to carry traffic for multiple VSANs.
- Fx ports:
  - An F_Port (fabric port) connects to an N_Port (end node port) on a host node through a point-to-point link.
  - An Fl_Port (fabric loop port) connects to an NL_Port (end node loop port) on a public loop through a point-to-point link or an arbitrated loop.
- A TL (translative loop) port may be connected to one or more private loop devices (NL ports). TL ports are unique to Cisco MDS 9000 Family switches and have similar properties to FL ports. The default is Auto, so the switch will autonegotiate the port speed.

For further information about port types, refer to the *Cisco 9000 Family Configuration Guide*.

Procedures for enabling, disabling, configuring, and viewing port attributes and statistics include:

Enabling or Disabling Ports

To enable a port, right-click on a disabled port in Device Manager and choose **Enable** from the pop-up menu.

To disable a port, right-click on a enabled port in Device Manager and choose **Disable** from the pop-up menu.

To enable or disable multiple ports, Ctrl-click each port or drag the mouse around a group of ports. Then right-click any of the selected ports and click either **Enable** or **Disable** from the pop-up menu.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Managing Interface Attributes for Ports

To manage port interface attributes from the Fabric Manager, choose **Physical Interfaces** from the menu tree and then choose one of the following port types to be configured:

- Port Channels
- xEPorts
- FxPorts
- Other Ports

To manage port interface attributes from the Device Manager, select a port on a module, and then choose a port type from the Interface menu.

The Fabric Manager Information pane displays interface attributes for multiple switches. The dialog box from Device Manager displays interface attributes for a single switch.

Viewing FLOGI Attributes

To view fabric login (FLOGI) attributes, such as the Fibre Channel ID (FCID), port name, and class of service for FxPorts from the Fabric Manager, choose **FC > Physical Interfaces** on the menu tree, and click the **FLOGI** tab.

To view FLOGI attributes from the Device Manager, choose **FxPorts** or **All Ports** from the Interface menu and click the **FLOGI** tab.

The Information pane in Fabric Manager displays attributes for multiple switches. The dialog box from Device Manager displays attributes for a single switch.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Viewing Port ELP Attributes

To monitor exchange link parameter (ELP) attributes, such as port and node world wide names and class of service from the Fabric Manager, choose **FC > Physical Interfaces** from the menu tree and click the **ELP** tab.

To monitor these attributes from the Device Manager, choose **xEPorts** or **All Ports** from the Interface menu and click the **ELP** tab.

The Information pane in Fabric Manager displays attributes for multiple switches. The dialog box from Device Manager displays attributes for a single switch.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Viewing Trunk Configuration

To monitor trunking for ports from the Fabric Manager, choose **FC > Physical Interfaces** from the menu tree, and then click the **Trunk Failures** tab.

To view trunking for ports from the Device Manager, choose **xEPorts** from the Interface menu and then click the **Trunk Failures** tab.

The Information pane in Fabric Manager displays attributes for multiple switches. The dialog box from Device Manager displays attributes for a single switch.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Managing Physical Attributes for a Port

To configure beacon mode and monitor physical attributes for ports from the Fabric Manager, choose **Physical Interfaces** from the menu tree and click the **Physical** tab.

To configure beacon mode and monitor physical attributes for ports from the Device Manager, choose the type of port from the Interface menu and click the **Physical** tab.

The Information pane in Fabric Manager displays attributes for multiple switches. The dialog box from Device Manager displays attributes for a single switch.

To enable or disable beacon mode, check the **BeaconMode** check box. When beacon mode is enabled, an interface LED flashes to identify the interface.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Viewing Port Capability Attributes

To monitor port capability attributes, such as buffer-to-buffer credit, hold time, and class of service from the Fabric Manager, choose **Physical Interface** from the menu tree and click the **Capability** tab.

To monitor these attributes from the Device Manager, choose the type of port from the Interface menu and click the **Capability** tab.

The Information pane in Fabric Manager displays attributes for multiple switches. The dialog box from Device Manager displays attributes for a single switch.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Managing PortChannel Interfaces

PortChanneling, also called port bundling, is the aggregation of multiple physical ports into one logical port to provide higher bandwidth, load balancing, and link redundancy. The Fabric Manager allows you to configure and monitor PortChannel interfaces on multiple Cisco 9000 switches. The Device Manager allows you to configure and monitor PortChannel interfaces on a single Cisco 9000 switch.

Procedures for configuring PortChannel interfaces using the Fabric Manager and the Device Manager include:

Managing PortChannel General Attributes

To manage PortChannels from the Fabric Manager, choose **Switches** > **PortChannels** from the menu tree. The Information pane in Fabric Manager displays attributes for multiple switches.

To manage PortChannels from the Device View, choose **PortChannels** from the Interface menu. The dialog box from Device Manager displays attributes for a single switch.

To add ports to a PortChannel, click **Create**. You see the Create PortChannel dialog box.

To add members to the PortChannel, enter the IP address of the switch into the MemberList field. Identify the other options you want to use and click **OK**.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Managing PortChannel Interface Attributes

To manage PortChannel interface attributes, such as the port mode and trunking from the Fabric Manager, choose the **Switches** > **PortChannels** from the menu tree.

To manage PortChannel interface attributes from the Device Manager, choose **PortChannels** from the Interface menu and click the **Interfaces** tab.

The Information pane in Fabric Manager displays attributes for multiple switches. The dialog box from Device Manager displays attributes for a single switch.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Monitoring Port Statistics

You can use Device Manager to monitor different types of port statistics. These options are available on the Interface menu from Device Manager's Device View or Summary View.

Procedures for monitoring port statistics include:

Monitoring and Charting Traffic Statistics

To monitor port traffic, discards, and errors for ports from the Device Manager, right-click on one or more ports and choose **Monitor Selected** from the Interface menu or right-click on one or more ports and choose **Monitor** from the pop-up menu. The the Monitor Traffic Statistics dialog box is displayed.

You can change the display by changing the following attributes from the Monitor Selected dialog box:

- Interval—Specifies the polling interval for the display in seconds, minutes, hours.
- AbsoluteValue—The actual counter value for the interface.
- Cumulative—The difference between the original absolute value and the last value retrieved for the interface.
- Average/sec —The average last value since the category was first displayed.
- Minimum/sec—The smallest last value.
- Maximum/sec—The largest last value.
- LastValue/sec—The difference between the current and previous counter values, normalized to per/second.

To display a line, area, or bar chart graph, select a traffic statistic and click one of the chart icons on the left side of the dialog box.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Monitoring Port Traffic (Bytes)

To monitor port traffic bytes from the Device Manager, choose the **Port Traffic (Bytes)** tab from the Port Monitor dialog box.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Monitoring Port Traffic (Frames)

To monitor port traffic frames from the Device Manager, choose the **Port Traffic (Frames)** tab on the Monitor Selected dialog box.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Monitoring Port Discards

To monitor port discards from the Device Manager, click the **Discards** tab on the Monitor Selected dialog box.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Monitoring Port Class 2 Errors

To monitor port class 2 errors from the Device Manager, click the **Class 2 Errors** tab on the Monitor Selected dialog box.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Monitoring Port Link Errors

To monitor port link errors from the Device Manager, click the **Link Errors** tab on the Monitor Selected dialog box.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Monitoring Port Sequence Errors

To monitor port sequence errors from Device Manager, click the **Seq Errors** tab on the Monitor Selected dialog box.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Monitoring Port Frame Errors

To monitor port frame errors from Device Manager, click the **Frame Errors** tab on the Monitor Selected dialog box.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Monitoring FICON

To monitor port frame errors from Device Manager, click the **FICON** tab on the Monitor Selected dialog box.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Managing PortChannels

To create a PortChannel from Fabric Manager, click on the PortChannel wizard icon in the Fabric Manager toobar.

To add a link to an existing PortChannel, right-click an ISL on the Fabric Manager map and select **Add to PortChannel** from the pop-up menu. The PortChannel wizard is displayed.

Note To create a PortChannel, all the ports on both ends of the link must have the same port speed, trunking type, and administrative state.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Managing Port Security

To configure Port Security from the Fabric Manager, you select Port Security from one of the VSANs shown in the Logical tab of the menu tree. Port Security is VSAN-based, and consists of the following steps:

- Identify the WWN of the ports that need to be secured

- Bind the fWWN to an authorized nWWN or pWWN
- Activate the port binding database for the required VSAN
- Enable auto-learning

The list below shows the Port Security tasks you can perform with Fabric Manager.

Turning AutoLearning On or Off

To turn AutoLearning on or off, perform the following steps.

Step 1 From the Fabric Manager, choose **Port Security** from one of the VSANs on the menu tree.

The information pane of the Fabric Manager displays Port Security information for that VSAN.

Step 2 Click the **Action** tab.

The switches for that VSAN are displayed.

Step 3 Click in the **AutoLearn** column next to the switch for which you want to enable AutoLearning.

A drop-down menu is displayed, with the selections **on** and **off**.

Step 4 Select **on** to turn on AutoLearning; select **off** to turn off AutoLearning for that switch.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Activating a Port Binding

To activate a Port Security port binding, perform the following steps.

Step 1 From the Fabric Manager, choose **Port Security** from one of the VSANs on the menu tree.

The information pane of the Fabric Manager displays Port Security information for that VSAN.

Step 2 Click the **Action** tab.

The switches for that VSAN are displayed.

Step 3 Click in the **Action** column under **Activation**, next to the switch for which you want to activate a port binding.

A drop-down menu is displayed, with the following selections:

activate - valid port bindings are activated

activate (TurnLearningOff) - valid port bindings are activated and autolearn turned off

forceActivate - activation is forced

forceActivate(TurnLearningOff) - activation is forced and autolearn is turned off

deactivate - deactivates all currently active port bindings

NoSelection - no action is taken

Step 4 Select the option you want to specify a port binding action for that switch.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Copying an Active Configuration to the Running Configuration

To turn AutoLearning on or off, perform the following steps.

Step 1 From the Fabric Manager, choose **Port Security** from one of the VSANs on the menu tree.

The information pane of the Fabric Manager displays Port Security information for that VSAN.

Step 2 Click the **Action** tab.

The switches for that VSAN are displayed.

Step 3 Click in the **CopyActive ToConfig** checkbox next to the switch for which you want to copy the configuration.

The active configuration is copied to the running configuration when the binding is activated.

Step 4 Uncheck the checkbox if you do not want the configuration copied when the binding is activated.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Configuring a Port Binding

To configure a port binding on a switch, perform the following steps.

Step 1 From the Fabric Manager, choose **Port Security** from one of the VSANs on the menu tree.

The information pane of the Fabric Manager displays Port Security information for that VSAN.

Step 2 Click the **Config** tab.

The Port Security configured port bindings for that VSAN are displayed.

Step 3 Click the Create Row icon.

The Create Binding dialog box is displayed.

Step 4 Select the switch from the dropdown list for which you want to create the port binding.

Step 5 Select the WWN DEVICE device type for that switch.

Step 6 Enter the PORT ID of the switch to bind to.

Step 7 Enter the port type.

Step 8 Enter the Interface (e.g. fc1/1)

Step 9 Click **Create** to creating the port binding, or click **Close** to close the Create Binding dialog without creating a port binding.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Deleting a Port Binding

To delete a port binding on a switch, perform the following steps.

Step 1 From the Fabric Manager, choose **Port Security** from one of the VSANs on the menu tree.

The information pane of the Fabric Manager displays Port Security information for that VSAN.

Step 2 Click the **Config** tab.

The Port Security configured port bindings for that VSAN are displayed.

Step 3 Click the row you want to delete.

Step 4 Click the Delete Row icon.

The confirmation dialog is displayed. Click Yes to delete the row, click No to close the confirmation dialog without deleting.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Displaying Activated Port Bindings

To display Port Security Active Port Bindings, perform the following steps.

Step 1 From the Fabric Manager, choose **Port Security** from one of the VSANs on the menu tree.

The information pane of the Fabric Manager displays Port Security information for that VSAN.

Step 2 Click the **Active** tab.

The Port Security active port bindings for that VSAN are displayed.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Displaying Port Security Statistics

To display Port Security Statistics, perform the following steps.

Step 1 From the Fabric Manager, choose **Port Security** from one of the VSANs on the menu tree.

The information pane of the Fabric Manager displays Port Security information for that VSAN.

Step 2 Click the **Statistics** tab.

The Port Security statistics for that VSAN are displayed.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Displaying Port Security Violations

Port violations are invalid login attempts (for example, login requests from unauthorized Fibre Channel devices). You can display a list of these attempts on a per-VSAN basis, using Fabric Manager. To display Port Security Violations, perform the following steps.

Step 1 From the Fabric Manager, choose **Port Security** from one of the VSANs on the menu tree.

The information pane of the Fabric Manager displays Port Security information for that VSAN.

Step 2 Click the **Violations** tab.

The Port Security violations for that VSAN are displayed.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

CHAPTER 9

Managing Zones and Zone Sets

The Fabric Manager allows you to configure and monitor zones and zone sets (groups of zones) on the Cisco MDS 9000 Family switch. Zoning allows you to set up access control between hosts and storage devices. You can use zones to control access between devices or user groups, and to increase network security and prevent data loss or corruption.

Note Zones and zone sets can only be created and configured using Fabric Manager, not Device Manager.

To verify the compatibility of the zone configuration on two connected switches, see "Analyzing the Results of Merging Zones" section on page 2-14. For information about zones and zone sets, and configuring them using the command-line interface (CLI), refer to the *Cisco 9000 Family Configuration Guide*.

Fabric Manager allows you to manage two types of zones and zonesets: regular, and inter-vsan (IVR) zones. Procedures to manage zones (regular and read-only) and zonesets include:

Procedures for managing Inter-VSAN (IVR) zones include:

The Zone Wizard can be used for either regular or IVR zones.

Creating Zones and Zonesets

Zones are configured within VSANs, but you can configure zones without configuring any VSANs by configuring them within the default VSAN. The Logical tab displays the VSANs configured in the currently discovered fabric. Note that zone information must always be identical for all the switches in the network fabric.

To create zones, zone sets, perform the following steps.

Step 1 From the Fabric Manager, choose **Zone > Edit Full Database on Switch** from the Fabric Manager **Zone** menu, or right-click a VSAN folder in the Logical tab and choose **Edit Local Zone Database** from the pop-up menu.

If you chose Zone > Edit Full Database on Switch, then the **Select VSAN** dialog is displayed. Select the VSAN and click OK.

The **Edit VSANxxx Local Full Zones** window is displayed for the VSAN you selected.

Step 2 Right click the Zoneset or Zone for that VSAN and selected Insert to add a Zoneset or Zone.

If you are adding a Zone, you can specify that the zone be a read-only zone by checking the **Set Zone as Read Only** checkbox. (For more information on read-only zones, see Read-Only Zones, page 9-3.)

If you are adding a ZoneSet, you can activate it by clicking the **Activate** button. This configuration is distributed to the other switches in the network fabric.

Note When you confirm the activate operation, the current running configuration is saved to the startup configuration. This permanently saves any changes made to the running configuration (not just zoning changes).

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Creating Additional Zones and Zonesets

To create additional zones and zone sets, follow these steps:

Step 1 With the **Edit Full Database on Switch** dialog open, right-click the **Zones** folder and choose **Insert** from the pop-up menu.

Step 2 Enter the zone name in the dialog box that appears and click OK to add the zone.

The zone is automatically added to the zone database.

Step 3 To create a zoneset, right-click the **ZoneSets** folder in the **Edit Full Database on Switch** dialog box, and choose **Insert**.

Step 4 Enter the zoneset name in the dialog box that appears and click OK to add the zoneset.

The zoneset is automatically added to the zone database.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Read-Only Zones

Read-only zones are implemented in Create Zone and View Zone. If the switch is running less than 1.2, the read only does not show. In read-only zoning, there is a flag in the SCSI header that is set for commands that can result in writing data to the storage. When read-only zoning is configured, relevant frames which have this bit set are trapped and are responded to from the switch. They don't reach the storage.

If a Windows 2000 server using the NTFS file system belongs to a read-only zone, it won't be able to mount the read-only zoned volume, and will not be able to read from or write to this volume. Currently, Windows 2000 servers with an NTFS file system are the only ones that do not support a read-only mount option. Solaris, Linux and Windows with a FAT32 file system do support the read-only mount option.

When read-only zoning is used, it is recommended that the server mounting the read-only volume have only read permission on that volume. If so, then read-only zoning enforces the expected read-only behavior from that server. If the volume permission is not set to read-only, then the read-only permission would also be enforced by the read-only zone; however, the host operating system is then unaware that it doesn't have write permission to the volume and its writes will fail. You would only know about this failure when the operating system tries to flush the cache, if caching is turned on.

On the other hand, if the volume permission is set to read-only from the operating system. then any write attempt will fail immediately.

Setting Default Zone Policy

Each VSAN contains a default zone, which by default, contains all connected devices assigned to the VSAN.

You can change the default zone policy for any VSAN by choosing **VSANxxx > Default Zone** from the Fabric Manager menu tree and clicking the **Policies** tab. However, we recommend that you establish connectivity among devices by assigning them to a nondefault zone.

The active zone set is shown in italic type. After you have made changes to the active zone set and before you activate the changes, the zone set is shown in boldface italic type. The tooltip for each zone indicates the activation time or modification time.

Adding Zones to a Zone Set

To add a zone to a zone set from the **Edit Full Database on Switch** window, drag and drop the zone to the folder for the zone set. Alternatively, follow these steps:

Step 1 Click the **ZoneSets** folder and then right-click the folder for the zone set to which you want to add a zone and choose **Insert** from the pop-up menu.

You see the Zone Server Select Zone dialog box.

Step 2 Select the zone that you want to add to the zone set and click **Add**.

The zone is added to the zone set in the zone database.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Cloning Zones and Zone Sets

Another method of adding zones and zone sets is to clone existing zones and zone sets. To clone a zone or zone set from the **Edit Full Database on Switch** window, follow these steps:

Step 1 Click the **Zones** or **ZoneSets** folder, right-click the folder for the zone or zone set that you want to clone, and choose **Clone** from the pop-up menu.

Step 2 Enter the name of the cloned zone or zone set.

By default, the dialog displays the selected zone as ClonedZone1.

Step 3 Click **OK** to add the cloned zone to the zone database.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Adding Zone Members

Once you have created a zone, you can add members to the zone. You can add members using the following port identification types:

- pWWN—The world wide name of the port configured on the end device (in hex format).
- Fabric port WWN—The world wide name of the physical port on the switch (in hex format).
- FC alias—The alias name in alphabetic characters (for example, Payroll).
- LUN—The logical unit number of a disk in a disk device.

For more information about port identification types, refer to the *Cisco 9000 Family Configuration Guide*.

To add members to a zone, follow these steps:

Step 1 Click the Zones folder, then right-click the folder for the zone to which you want to add members, and choose **Insert** from the pop-up menu.

The Add Members to Zone dialog is displayed.

Step 2 Click the checkbox to the left of the NxPort WWN field.

Step 3 Select one of the ports in the VSAN and click **Add** to add it to the zone.

You see member in the Zone Server database in the lower frame.

Step 4 Repeat these steps to add other members to the zone.

Note When configuring a zone member, you can specify that a single LUN can have multiple IDs depending on the operating system. You can select from 6 different operating systems.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Activating or Enforcing Zone Sets

Once zones and zone sets have been created and populated with members, you must activate or enforce the zone set. Note that only one zone set can be activated at any time. If zoning is activated, any member that is not assigned to an active zone belongs to the default zone. If zoning is not activated, all members belong to the default zone.

To activate a zone set, follow these steps:

Step 1 Right click the zone set in the **Edit Full Database on Switch** dialog box.

Step 2 Click **Activate**.

You see the zone set in the Active Zone Set folder.

Note If one zone set is active and you activate another zone set, the currently active zone set is automatically deactivated.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Deactivating Zonesets

To activate a zone set, follow these steps:

Step 1 Right click the zone set in the **Edit Full Database on Switch** dialog box.

Step 2 Click **Deactivate**.

You see the zone set removed from the Active Zone Set folder.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Viewing Aliases

Aliases are assigned per port. To view zone aliases, follow these steps:

Step 1 From the Fabric Manager, choose **Zone > Edit Full Database on Switch** from the Fabric Manager **Zone** menu, or right-click a VSAN folder in the Logical tab and choose **Edit Local Zone Database** from the pop-up menu.

If you chose Zone > Edit Full Database on Switch, then the **Select VSAN** dialog is displayed. Select the VSAN and click OK.

The **Edit VSANxxx Local Full Zones** window is displayed for the VSAN you selected.

Step 2 Click the Aliases tab to see the aliases for that zone.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Displaying Port Membership Information

To display port membership information for members assigned to zones, perform the following steps.

Step 1 From the Fabric Manager, choose **Zone > Edit Full Database on Switch** from the Fabric Manager **Zone** menu, or right-click a VSAN folder in the Logical tab and choose **Edit Local Zone Database** from the pop-up menu.

If you chose Zone > Edit Full Database on Switch, then the **Select VSAN** dialog is displayed. Select the VSAN and click OK.

The **Edit VSANxxx Local Full Zones** window is displayed for the VSAN you selected.

Step 2 Click the **Members** tab.

Note The default zone members are explicitly listed only when the default zone policy is configured as **permit**. When the default zone policy is configured as **deny**, the members of this zone are not shown. For more information, see the "Changing the Default Zone Policy" section on page 9-8.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Deleting Zones, Zone Sets, and Members

To delete zones, zone sets, or members, perform the following steps.

Step 1 From the Fabric Manager, choose **Zone > Edit Full Database on Switch** from the Fabric Manager **Zone** menu, or right-click a VSAN folder in the Logical tab and choose **Edit Local Zone Database** from the pop-up menu.

If you chose Zone > Edit Full Database on Switch, then the **Select VSAN** dialog is displayed. Select the VSAN and click OK.

The **Edit VSANxxx Local Full Zones** window is displayed for the VSAN you selected.

Step 2 Select the Zone, Zone Set, or Member you want to delete.

Step 3 Right-click the object and choose **Delete** from the pop-up menu.

The selected object is deleted from the zone database.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Changing the Default Zone Policy

Each member in the fabric can belong to any zone. If a member does not belong to any zone, it is part of the default zone. If no zone has been activated in the fabric, all members belong to the default zone. Even though a member can belong to multiple zones, a member in the default zone cannot be part of any other zone.

Traffic can be permitted and denied to members in the default zone. This information is not distributed to all switches. Permission and denial must be set for each switch in the fabric.

To permit or deny traffic to members in the default zone from the Zone Server, follow these steps:

Step 1 Choose **VSANxxx > Default Zone** from the Fabric Manager menu tree, and click the **Policies** tab.

The Zone information is displayed in the Information pane.

Step 2 Click the **DefaultZoneBehavior** field and choose either **permit** or **deny** from the pull-down menu.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Viewing Zone Statistics

To monitor zone statistics from the Zone Server, choose **VSANxxx > Domain Manager** from the Fabric Manager menu tree. The Zone information is displayed in the Information pane. Click on the **Statistics** tab to see the statistics information for the switches in the zone.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Importing Active Zonesets

You can import active zonesets (do a Merge Fail Recovery) if the cause of an ISL failure is a zone merge fail. To import an active zoneset, perform these steps.

Step 1 From the Fabric Manager, choose **Zone > Merge Fail Recovery** from the Fabric Manager **Zone** menu.

The **Zone Merge Failure Recovery** dialog is displayed.

Step 2 Select the Import Active Zoneset radio button.

Step 3 Select the switch from which to import the Zoneset information, from the dropdown list.

Step 4 Select the VSAN from which to import the Zoneset information, from the dropdown list.

Step 5 Select the interface to use for the import process.

Step 6 Click OK to import the active zoneset, or click Close to close the dialog without importing the active zoneset.

Exporting Active Zonesets

You can export active zonesets (do a Merge Fail Recovery) if the cause of an ISL failure is a zone merge fail. To export an active zoneset, perform these steps.

Step 1 From the Fabric Manager, choose **Zone > Merge Fail Recovery** from the Fabric Manager **Zone** menu.

The **Zone Merge Failure Recovery** dialog is displayed.

Step 2 Select the Export Active Zoneset radio button.

Step 3 Select the switch to which to export the Zoneset information, from the dropdown list.

Step 4 Select the VSAN to which to export the Zoneset information, from the dropdown list.

Step 5 Select the interface to use for the export process.

Step 6 Click OK to export the active zoneset, or click Close to close the dialog without exporting the active zoneset.

Performing Zone Merge Analysis

To perform a zone merge analysis, perform these steps.

Step 1 From the Fabric Manager, choose **Zone > Merge Analysis** from the Fabric Manager **Zone** menu.

The **Zone Merge Analysis** window is displayed.

Step 2 Select the first switch to be analyzed from the **Check Switch 1** dropdown list.

Step 3 Select the second switch to be analyzed from the **And Switch 2** dropdown list.

Step 4 Enter the VSAN ID where the zoneset merge failure occured, in the **For Active Zoneset Merge Problems in VSAN** field.

Step 5 Click Analyze to analyze the zone merge. Click Clear to clear the analysis data from the Zone Merge Analysis window. If you click Analyze without clicking Clear, the new zone merge analysis data is displayed below the old data.

Recovering a Full Zone Database

You can recover a database by copying the active zone database or the full zone database. To recover a zone database, perform these steps.

Step 1 From the Fabric Manager, choose **Zone > Recover Full Zone Database** from the Fabric Manager **Zone** menu.

The **Recover Full Zone Database** dialog is displayed.

Step 2 Select the Copy Active or the Copy Full radio button, depending on which type of database you want to copy.

Step 3 Select the source VSAN from which to copy the information, from the dropdown list.

Step 4 If you selected Copy Full, select the source switch and the destination VSAN from those dropdown lists.

Step 5 Select the destination switch from the dropdown list.

Step 6 Click Copy to Copy the database, or click Close to close the dialog without copying.

Migrating a Non-MDS Database

You use the Zone Migration Wizard to migrate a non-MDS database.

Step 1 From the Fabric Manager, choose **Zone > Migrate Non-MDS Database** from the Fabric Manager **Zone** menu.

The **Zone Migration Wizard** is displayed.

Step 2 Follow the prompts in the wizard to migrate the database.

IVR Zones and Zonesets

Initiators and targets in different VSANs are completely isolated from each other. Inter-VSAN Routing (IVR) bridges that gap by selectively allowing devices to selectively transfer data across VSANs. The Cisco MDS 9000 family of switches supports IVR.

In IVR, source and destination VSANs are separated by zero or more “transit” VSANs. A transit VSAN is a VSAN used to provide a route between two VSANs. This requires that domain IDs across interconnected VSANs are unique. Cisco MDS switches running a MDS SAN-OS version lower than 1.3(1) will continue to work as before. IVR is transparent to third-party switches.

VSAN topology information allows the computation of shortest inter-vsan route(s). IVR will load balance across these shortest paths, if there is more than one path. Load balancing works within a VSAN as well as across VSANs, and in-order delivery is maintained.

Inter-VSAN Zoning

An Inter-VSAN Zone (IVZ) defines a set of end-nodes allowed to communicate across VSANs. Membership is specified by both pwwn and VSAN ID. Inter-VSAN Zones (IVZs) and Inter-VSAN Zonesets (IVZSs) are configured in parallel with intra-VSAN zones/zoneset. However, their configurations are independent of each other. Active IVZs become part of the regular zone when activated, and are listed under the VSAN with the regular zones. Like intra-VSAN zonesets, there can be only one active IVZS.

IVZ Configuration Process Overview

Cisco Fabric Manager provides a wizard to help you set up Inter-VSAN zones, or you can do it manually. The process is:

- Enable IVR on each relevant gateway switch. IVR need not be *enabled* at all IVR-capable border switches - only switches at VSAN borders need to be IVR-enabled. Ensure that domain IDs are unique amongst switches/VSANs participating in IVR. Each switch will then be able to build an internal graph of inter-VSAN routes.
- Cisco Fabric Manager chooses a reference switch, from which the configuration will be copied to other IVR-enabled switches. The reference switch that is chosen is the closest available IVR switch. If there are no IVR switches, you must enable one from the available switches running MDS SAN-OS 1.3(1) or higher. Set up the information on this reference switch so that it is correct, and can be propagated to the other relevant IVR-enabled border switches. It is important that the information on each of these switches is identical. The copy process removes any previous zone configuration that was enabled on the IVR switches.
- Configure and activate VSAN topology on these IVR-enabled border switches. (The dropdown list to activate the switches shows only the IVR-enabled switches, and these switches must be activated in parallel.) You must explicitly specify the VSANs available at each IVR-enabled switch (the “VSAN Topology”).
- Activate the Zoneset. IVR configuration needs to be activated at each IVR-enabled border switch

Please keep the following notes in mind when creating IVR zones and zonesets:

Note Some time zones beginning with prefix 'IVRZ' and a zoneset with name 'nozoneset' appear in logical view. The zones with prefix 'IVRZ' are IVR zones which get appended to regular active zones. The prefix 'IVRZ' is appended to active IVR zones by the system. Similarly the zoneset with name 'nozonset'

is an IVR active zoneset created by system if no active zoneset is available for that vsan and if 'ivrZoneSetActivateForce' flag is enabled on switch. In server.properties file you can set the property zone.ignoreIVRZones to true or false to either hide or view IVR zones as part of regular active zones. Do not create a zone with prefix 'IVRZ' or a zoneset with name 'nozonset'. These names are used by the system for identifying IVR zones.

Creating IVR Zones and Zonesets

To create IVR zones or zone sets, perform the following steps.

Step 1 From the Fabric Manager, choose **Zone > IVR (Inter VSAN Routing) > Edit Full Database on Switch** from the Fabric Manager **Zone** menu.

The **Edit VSANxxx Local Full Zones** window is displayed for the VSAN you selected.

Step 2 Right click the Zoneset or Zone for that VSAN and selected Insert to add a Zoneset or Zone.

If you are adding a ZoneSet, you can activate it by clicking the **Activate** button. This configuration is distributed to the other switches in the network fabric.

Note When you confirm the activate operation, the current running configuration is saved to the startup configuration. This permanently saves any changes made to the running configuration (not just zoning changes).

Note Some time zones beginning with prefix 'IVRZ' and a zoneset with name 'nozoneset' appear in logical view. The zones with prefix 'IVRZ' are IVR zones which get appended to regular active zones. The prefix 'IVRZ' is appended to active IVR zones by the system. Similarly the zoneset with name 'nozonset' is an IVR active zoneset created by system if no active zoneset is available for that vsan and if 'ivrZoneSetActivateForce' flag is enabled on switch. In server.properties file you can set the property zone.ignoreIVRZones to true or false to either hide or view IVR zones as part of regular active zones.

Note Do not create a zone with prefix 'IVRZ' or a zoneset with name 'nozonset'. These names are used by the system for identifying IVR zones.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Creating Additional IVR Zones and Zonesets

To create additional zones and zone sets, follow these steps:

Step 1 With the **Zone > IVR (Inter VSAN Routing) > Edit Full Database on Switch** dialog open, right-click the **Zones** folder and choose **Insert** from the pop-up menu.

Step 2 Enter the zone name in the dialog box that appears and click OK to add the zone.

The zone is automatically added to the zone database.

Step 3 To create a zoneset, right-click the **ZoneSets** folder in the **Edit Full Database on Switch** dialog box, and choose **Insert**.

Step 4 Enter the zoneset name in the dialog box that appears and click OK to add the zoneset.

The zoneset is automatically added to the zone database.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Activating IVR Zonesets

Once the zone sets have been created and populated, you must activate the zone set. To activate an IVR zone set, follow these steps:

Step 1 Right click the zone set in the **Zone > IVR (Inter VSAN Routing) > Edit Full Database on Switch** dialog box.

Step 2 Click **Activate**.

Note The active zoneset in Edit Zone is always shown in bold, even after successful activation. This is because a member of this vsan must be participating in IVR zoning. Since the IVR zones get added to active zones, the active zoneset configuration is always different from local zoneset configuration with same name.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Deactivating IVR Zonesets

To activate a zone set, follow these steps:

Step 1 Right click the zone set in the **Zone > IVR (Inter VSAN Routing) > Edit Full Database on Switch** dialog box.

Step 2 Click **Deactivate**.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Recovering an IVR Full Zone Database

You can recover an IVR zone database by copying the IVR full zone database. To recover an IVR zone database, perform these steps.

Step 1 From the Fabric Manager, choose **Zone > IVR (Inter VSAN Routing) > Recover Full Zone Database** from the Fabric Manager **Zone** menu.

The **Recover Full Zone Database** dialog is displayed.

Step 2 Select the Copy Active or the Copy Full radio button, depending on which type of database you want to copy.

Step 3 Select the source VSAN from which to copy the information, from the dropdown list.

Step 4 If you selected Copy Full, select the source switch and the destination VSAN from those dropdown lists.

Step 5 Select the destination switch from the dropdown list.

Step 6 Click Copy to Copy the database, or click Close to close the dialog without copying.

Recovering an IVR Full Topology

You can recover a topology by copying the active zone database or the full zone database. To recover a zone database, perform these steps.

Step 1 From the Fabric Manager, choose **Zone > IVR (Inter VSAN Routing) > Recover FullTopology** from the Fabric Manager **Zone** menu.

The **Recover Full Topology** dialog is displayed.

Step 2 Select the Copy Full radio button.

Step 3 Select the source VSAN from which to copy the information, from the dropdown list.

Step 4 Select the source switch and the destination VSAN from those dropdown lists.

Step 5 Select the destination switch from the dropdown list.

Step 6 Click Copy to Copy the topology, or click Close to close the dialog without copying.

Using the Zone Wizard

You use the Zone Wizard to configure zones, read-only zones, and IVR zones.

Step 1 From the Fabric Manager, choose **Zone > Zone Wizard** from the Fabric Manager **Zone** menu.

The **Zone Wizard** is displayed.

Step 2 Follow the prompts in the wizard to migrate the database.

CHAPTER 10

Managing Administrator Access

The Cisco Fabric Manager lets you control management access to Cisco MDS 9000 Family switches, whether you are using the command-line interface (CLI) or SNMP. The Cisco Fabric Manager uses SNMP to communicate remotely with switches.

SNMP v3 provides a security model for controlling management access to managed devices in the form of a set of users and roles. Users are assigned to specific roles, and specific administrative privileges are assigned to each role. User names are authenticated through passwords, which are stored and transmitted in encrypted form. In addition, SNMPv3 includes the Privacy option, which encrypts all management traffic exchanged between switches.

SNMP v1 and v2 provide a very limited authentication scheme in the form of read and write community strings. Community strings are like user names, without passwords, and are stored and sent over the SNMP network in clear text (unencrypted) form. For this reason, SNMPv3 should be used wherever network security is a concern.

Procedures for managing SNMP users and roles, which allow you to control remote administrative access to Cisco MDS 9000 Family switches, include:

You can also set up a RADIUS server to provide authentication services to CLI users. To remotely access switches using the CLI, you use Telnet or SSH. For information about managing remote CLI access or configuring a local database for authenticating CLI users, refer to the *Cisco 9000 Family Configuration Guide*.

Procedures for setting up a RADIUS server include:

Viewing SNMP Users, Roles, and Communities

To view information about SNMP users, roles, and communities from Fabric Manager, choose **Security > SNMP** from the menu tree and click the **Users** tab. The list of SNMP users, roles, and communities is displayed in the Information pane.

To view this information from the Device Manager, choose **SNMP** from the Security menu. The SNMP dialog box is displayed.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Adding a User or Community String

To add a user or community string, follows these steps:

Step 1 Click **Create** on the Device Manager dialog box, or click the **Create Row** button on the Fabric Manager toolbar.

The Create Community string dialog box is displayed.

The dialog box from Fabric Manager also provides check boxes to specify one or more switches.

Step 2 Enter the user name in the New User field.

Step 3 Select the role from the drop-down list.

Step 4 Enter the password for the user twice in the New Password and Confirm Password fields.

Step 5 Click the **Privacy** check box and complete the password fields to enable encryption of management traffic,

Enter the Authentication password in the Clone Password field to use the same password. Enter a new password twice in the New Password and Confirm Password fields.

Step 6 Click **Create** to create the new entry or click **Close** to create the entry and close the dialog box.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Configuring SNMP Communities

If you are running SNMPv3, you must define users (or security names), assign them to roles (or groups), and assign system access based on those roles. If you are running SNMPv1 or SNMPv2c, you must define communities, which are equivalent to SNMPv3 users or security names. SNMPv3 allows you to define user access to the object level. SNMPv1 and SNMPv2c do not allow you to define system access at the object level.

Table 10-1 shows the mapping of users (SNMPv3) and communities (SNMPv1 and SNMPv2c).

Table 10-1 SNMP Mappings

SNMPv3	SNMPv1, SNMPv2c
user or security name	community
role	role

To configure users and communities from the Device Manager, choose **SNMP** from the Security menu. and click the **Communities** tab. The SNMP dialog box with the Communities tab selected is displayed.

To configure users and communities from the Fabric Manager, choose **Security > SNMP** from the menu tree and click the **Communities** tab. The SNMP Communities information is displayed in the Fabric Manager Information pane.

To add a community string, follow these steps:

Step 1 Click **Create** on the Device Manager dialog box or click the **Create Row** button on the Fabric Manager toolbar.

The Create Community string dialog box is displayed.

The dialog box from Fabric Manager also provides a check box to specify one or more switches.

Step 2 Enter the community string in the Community field.

Step 3 Select the user role from the pull-down selection list.

Step 4 Click **Create**.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Configuring User Roles

User roles let you define a set of administrative permissions for a role and then assign this role to different users.

To configure users roles, choose **SNMP** from the Device Manager Security menu, and click the **Roles** tab.

To create a new role, follow these steps:

Step 1 Click **Create**.

The system displays the Create Roles dialog box.

Step 2 Enter an identifier for the role in the Role field.

Step 3 Select one of the following security levels:

authNoPrv—Authentication without encryption

AuthPriv—Authentication with encryption

Step 4 For Read access, click the **All** radio button to enable full read access or click **List** and click each check box in the list to enable read access to specific information.

Step 5 For Write access, click the **All** radio button to enable full read access or click **List** and click each check box in the list to enable read access to specific information.

Step 6 Click **Apply** to create the new role or click **OK** to create the role and close the window.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Configuring Common Roles

Common Roles allow you to use a set of rules to set the scope of VSAN security. To configure Common Roles from the Device Manager, select Common Roles from the Security menu. You can then access the Rules dialog box to configure the set of rules. To configure Common Roles from Fabric Manager, select **Security > SNMP** and click the **Roles** tab in the Information pane. Fabric Manager uses a default rules set for roles; therefore, no Rules dialog box is displayed.

The list below shows the Common Roles tasks you can perform with Device Manager or Fabric Manager.

- Creating Common Roles, page 10-4
- Editing Common Role Rules (DM Only), page 10-5
- Deleting Common Roles, page 10-6

Creating Common Roles

To create a common role, perform the following steps.

Step 1 From the Device Manager, choose **Common Roles** from the **Security** menu. The Common Roles dialog box is displayed.

From Fabric Manager, select **Security > SNMP** from the menu tree, and click the **Roles** tab in the information pane.

Step 2 Click the **Create** button.

The Create Common Roles dialog box is displayed.

Step 3 From Fabric Manager, select the switches for which you want to configure the Common Role. If you are using Device Manager, skip to Step 4.

Step 4 Enter the name of the Common Role in the Name field.

Step 5 Enter the description of the Common Role in the Description field.

Step 6 From Fabric Manager, check (or uncheck) the **Has Config and Exec Permission** checkbox. If you are using Device Manager, skip to Step 7.

If you check the checkbox, your role will have read, write, and create permission. If you do not check the checkbox, your role will have read-only permission.

Step 7 Click **Enable** to enable the VSAN scope.

Step 8 Enter the scope in the Scope field.

Step 9 From Device Manager, click the **Rules** button to view the rules for the role, and select the rules you want to enable. Then click **Close** to close the Rules dialog. If you are using Fabric Manager, skip to Step 10.

The Rules dialog may take a few minutes to display.

Step 10 Click **Create** to create the common role, or click **Close** to close the Common Role dialog without creating the common role.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Editing Common Role Rules (DM Only)

To edit the rules for a common role, perform the following steps.

Step 1 From the Device Manager, choose **Common Roles** from the **Security** menu.

The Common Roles dialog box is displayed.

Step 2 Click once on the common role for which you want to edit the rules.

Step 3 Click the **Rules** button to view the rules for the role.

The Rules dialog may take a few minutes to display.

Step 4 Edit the rules you want to enable or disable for the common role.

Step 5 Click **Apply** to apply the new rules and close the Rules dialog, or click **Close** to close the Rules dialog without applying the rules.

Step 6 Click **Apply** to create the common role, or click **Close** to close the Common Role dialog without creating the common role.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Deleting Common Roles

To delete a common role, perform the following steps.

Step 1 From the Device Manager, choose **Common Roles** from the **Security** menu. The Common Roles dialog box is displayed.

From Fabric Manager, select **Security** > **SNMP** from the menu tree, and click the **Roles** tab in the information pane.

Step 2 Click once to select the common role you want to delete.

Step 3 Click the **Delete** button to delete the common role.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Configuring RADIUS Authentication

To configure RADIUS authentication from the Fabric Manager, choose **Security** > **Radius** from the menu tree.

To configure RADIUS authentication from the Device Manager, choose **Radius** (CLI) from the Security menu.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Configuring RADIUS Servers

To configure RADIUS servers, perform the following steps:

Step 1 From the Device Manager, choose **Radius** from the **Security** menu and click the **Servers** tab. The Radius dialog box with the Servers tab selected is displayed.

To configure RADIUS servers from the Fabric Manager, choose **Security> Radius** from the menu tree and click the **Servers** tab. The Radius information is displayed in the Information pane.

Step 2 To add a Radius server, click **Create** on the Device Manager dialog box, or click the **Create Row** button on the Fabric Manager toolbar.

The Create Radius Server dialog box is displayed. In Fabric Manager, you can specify the switches to which the configuration applies

Step 3 Complete the fields, and click **OK.**

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

CHAPTER 11

Managing IP Storage

Cisco MDS 9000 Family switches can route FCIP and iSCSI IP storage services independently, allowing servers to connect to a storage network using Fibre Channel or IP. Using open-standard IP-based technology, the Cisco MDS 9000 Family IP storage services enable you to interconnect remote SAN islands using FCIP, and to extend SAN connectivity to IP-enabled servers using iSCSI protocols.

Fabric Manager allows you to configure and monitor FCIP and iSCSI storage services on multiple Cisco 9000 switches. Device Manager allows you to configure and monitor these services on a single Cisco 9000 switch.

For information about configuring FCIP and iSCSI storage services using the command-line interface (CLI), refer to the *Cisco 9000 Family Configuration Guide*.

To learn more about managing IP storage services, refer to the following topics:

IP Storage Services Module

The IP Storage Services (IPS) module must be installed in your Cisco MDS 9000 Family switch before you can manage FCIP and iSCSI services on that switch. It integrates seamlessly into the Cisco MDS 9000 Family, and supports the full range of services available on the switching modules, including VSANs, security, and traffic management. Traffic can be forwarded between any IP storage port and any other port on a Cisco MDS 9000 Family switch.

The IPS module can be used in any Cisco MDS 9500 or 9200 series switch. The IPS module has eight SFP Gigabit Ethernet (Gig-E) ports, and it is hot-swappable. Each port can run FCIP and iSCSI protocols simultaneously.

- FCIP — FCIP transports Fibre Channel frames transparently over an IP network between two Cisco MDS 9000 Family switches or other FCIP standards-compliant devices.
- iSCSI — The IPS module provides IP hosts access to Fibre Channel storage devices. The IP host-initiated SCSI commands are encapsulated in IP and sent to a Cisco MDS 9000 port. At this point, the commands are routed from the IP network into a Fibre Channel network and forwarded to the intended target.

Managing Gigabit Ethernet Interfaces

The Gigabit Ethernet ports on the IPS module can only be used to perform IP storage services like iSCSI and FCIP. This port does not bridge ethernet frames or route IP packets. A new port mode option, **IPS mode**, is defined for Gigabit Ethernet ports. IP storage ports are implicitly set to IPS mode (so they only perform IP storage functionality). You can use an IPS module to perform either iSCSI or FCIP storage services.

The Gigabit Ethernet interface must be configured with an IP address before it can perform IP storage services functions. When one Cisco MDS 9000 Family switch connects to another Cisco MDS 9000 Family switch via the IPS modules, the following apply:

- The two switches are connected through a virtual ISL running on the FCIP tunnel. The endpoints of the virtual ISL are two virtual E ports.
- The virtual E ports become virtual TE ports if trunking is enabled, and the connecting link is a virtual EISL.

Refer to the *Cisco 9000 Family Configuration Guide* if there are problems.

Procedures for configuring Gigabit Ethernet interfaces include:

- Configuring Gigabit Ethernet Interfaces, page 11-3

Managing FCIP

Fibre Channel over TCP/IP (FCIP) is a service that allows islands of Fibre Channel SANs to be interconnected over IP networks to form a unified SAN — a single Fibre Channel fabric. These connections are referred to as "FCIP tunnels."

This section describes two ways to create FCIP tunnels. You can use the Device Manager, or you can use the FCIP Wizard to create tunnels using the Fabric Manager. See the "Creating FCIP Tunnels with Fabric Manager" section on page 11-6 for this information.

Procedures for creating and managing FCIP include:

- Assigning FCIP Profiles, page 11-4
- Creating Tunnels, page 11-4
- Verifying Interfaces, page 11-5
- Verifying Extended Link Protocols (ELP), page 11-5
- Checking Trunk Status, page 11-6
- Checking for Interface Errors, page 11-6

Managing iSCSI Services

Cisco MDS 9000 Family iSCSI storage services provide IP hosts with access to Fibre Channel storage devices as if each storage device were directly attached to the hosts. The switch transparently presents each IP host to the storage device as if each host were an Fibre Channel host. iSCSI services create virtual iSCSI targets and maps them to physical Fibre Channel targets available in the Fibre Channel SAN. It presents the iSCSI targets to IP hosts as if the physical targets were directly attached to the hosts.

In conjunction with presenting iSCSI targets to hosts, iSCSI Service presents each IP host as an Fibre Channel host, i.e. Host Bus Adaptor (HBA) to the storage device. The storage device is aware of each IP host and responds to each IP host as if it were an Fibre Channel host connected to the storage device.

For more information on iSCSI services, see the *Cisco 9000 Family Configuration Guide*.

Procedures for managing iSCSI include:

- Specifying Targets, page 11-7
- Specifying LUN Mappings, page 11-8
- Viewing iSCSI Statistics, page 11-8
- Viewing iSCSI Sessions, page 11-8
- Viewing Session Statistics, page 11-9
- Creating an iSCSI Initiator, page 11-9

Configuring Gigabit Ethernet Interfaces

Each port or interface on the IPS module is displayed in the Ethernet Port dialog.

To configure Ethernet port interfaces, do the following:

Step 1 Be sure you are connected to a switch that contains an IPS module.

Step 2 Open Device Manager.

Step 3 Select any Ethernet port by clicking on it once.

Step 4 Select Gigabit Ethernet Ports from the Interfaces menu. All Gigabit Ethernet ports for the switch are displayed in a table.

Step 5 To configure the alias, state, or IP address for a particular port, double-click on the appropriate table cell.

Step 6 Enter the alias, IP address, or state for the port.

Step 7 Click Apply.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Creating FCIP Tunnels with Device Manager

To create and manage FCIP tunnels with Device Manager, first verify that the IPS module is inserted in the required Cisco MDS 9000 Family switches, and that the switches' Gigabit Ethernet interfaces are connected and the connectivity verified using the **ping** command. The steps in creating FCIP tunnels are:

- Assigning FCIP Profiles, page 11-4
- Creating Tunnels, page 11-4
- Verifying Interfaces, page 11-5

Assigning FCIP Profiles

You can use Device Manager to configure FCIP tunnels between switches. First, you must create FCIP profiles, and then bind the interfaces to the profile. To bind an FCIP profile to an interface, use the IP address of the interface in the FCIP profile's IP address configuration. Profile numbers range from 1 to 255. The interface associated with a profile can be either of the following:

- EtherChannel
- Ethernet subinterface slot and port (or slot, port, and VLAN ID)

To create and bind profiles on a Gigabit Ethernet interface, follow these steps.

Step 1 Be sure you are connected to a switch that contains an IPS module.

Step 2 Open Device Manager.

Step 3 Select FCIP from the IP menu.

Step 4 Click the Profiles tab if it is not already selected. The FCIP Profiles dialog is displayed. Any profiles already bound, are listed in the table along with their IP addresses.

Step 5 To add a new profile, click Create. The Create FCIP Profiles dialog is displayed.

Step 6 Enter the profile ID in the ID field.

Step 7 Select an IP address of the interface to which you want to bind the profile from the IP Address dropdown list.

Step 8 Enter all the optional information, if desired.

Step 9 When finished, click Create to add this profile to the table. Click Close to exit the Create FCIP profiles dialog without adding the profile.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Creating Tunnels

Each Gigabit Ethernet interface can have 3 active FCIP tunnels on it at one time. To create these tunnels, do the following:

Step 1 Be sure you are connected to a switch that contains an IPS module.

Step 2 Open Device Manager.

Step 3 Select FCIP from the IP menu.

Step 4 Click the Tunnels tab if it is not already selected. The FCIP Tunnels dialog is displayed.

This table lists the remote IP address of the interface together with optional attributes.

Step 5 Click the Create button. The Create FCIP Tunnels dialog is displayed.

Step 6 Enter the entity ID in the ID field.

Step 7 Enter a remote IP address as the endpoint to which you want to link.

Step 8 Enter all the optional information, if desired.

Step 9 When finished, click Create to add this tunnel to the table. Click Close to exit the Create FCIP Tunnels dialog without adding the tunnel.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Verifying Interfaces

To verify the interfaces, do the following:

Step 1 Be sure you are connected to a switch that contains an IPS module.

Step 2 Open Device Manager.

Step 3 Select FCIP from the Interface menu.

Step 4 Click the Interfaces tab if it is not already selected. The FCIP Interfaces dialog is displayed.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Verifying Extended Link Protocols (ELP)

To verify the extended link protocol, do the following:

Step 1 Be sure you are connected to a switch that contains an IPS module.

Step 2 Open Device Manager.

Step 3 Select FCIP from the IP menu.

Step 4 Click the ELP tab if it is not already selected. The FCIP ELP dialog is displayed.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Checking Trunk Status

To check the trunk status, do the following:

Step 1 Be sure you are connected to a switch that contains an IPS module.

Step 2 Open Device Manager.

Step 3 Select FCIP from the IP menu.

Step 4 Click the Trunk Status tab if it is not already selected. The FCIP Trunk Status dialog is displayed.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Checking for Interface Errors

To check for interface errors, do the following:

Step 1 Be sure you are connected to a switch that contains an IPS module.

Step 2 Open Device Manager.

Step 3 Select FCIP from the IP menu.

Step 4 Click the Interface Errors tab if it is not already selected. The FCIP Interface Errors dialog is displayed, listing FCIP-specific end-point/interface errors.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Creating FCIP Tunnels with Fabric Manager

To create and manage FCIP tunnels with Fabric Manager, you use the FCIP Wizard. First verify that the IPS module is inserted in the required Cisco MDS 9000 Family switches, and that the switches' Gigabit Ethernet interfaces are connected and the connectivity verified. The steps in creating FCIP tunnels using the FCIP Wizard are:

- select the endpoints
- choose the interfaces' IP addresses
- specify link attributes

To create FCIP tunnels using the FCIP Wizard, follow these steps:

Step 1 Select the endpoints.

Step 2 Choose the ports' IP addresses.

Step 3 Select the link attributes.

Authenticating iSCSI Targets

To authenticate iSCSI targets, first specify the initiators. To specify initiators, perform the following steps:

Step 1 Be sure you are connected to a switch that contains an IPS module.

Step 2 Open Device Manager.

Step 3 Select iSCSI from the IP menu. The iSCSI dialog is displayed.

Step 4 Select the Initiators tab if it is not already selected.

This table lists iSCSI initiators, VSAN membership, and, if applicable, persistent node and port WWN addresses. Use the Create dialog is used to assign the VSAN and addresses.

Step 5 Click the Create button. The Create iSCSI Initiators dialog is displayed.

Step 6 Enter the initiator name in the Name field.

Step 7 Enter the VSAN membership number in the VSAN Membership field.

Step 8 Enter all the node and port information.

Step 9 When finished, click Create to add this initiator to the table. Click Close to exit the Create iSCSI initiators dialog without adding the initiator. Like physical N ports, iSCSI Initiators will appear in the Fabric Login Table.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Specifying Targets

To specify targets, perform the following steps:

Step 1 Be sure you are connected to a switch that contains an IPS module.

Step 2 Open Device Manager.

Step 3 Select iSCSI from the IP menu. The iSCSI dialog is displayed.

Step 4 Select the Targets tab if it is not already selected.

This table lists both statically assigned as well as dynamically discovered Fiber Channel targets. Use the import button to automatically discover and populate this table with existing targets. Use the Create button to assign port address or control iSCSI access to certain targets.

Step 5 Click the Create button. The Create iSCSI Targets dialog is displayed.

Step 6 Enter the target name in the Name field.

Step 7 Enter the Port WWN, node access information, and advertised interfaces information in the appropriate fields.

Step 8 When finished, click Create to add this target to the table. Click Close to exit the Create iSCSI Targets dialog without adding the target.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Specifying LUN Mappings

To specify LUN mappings, perform the following steps:

Step 1 Be sure you are connected to a switch that contains an IPS module.

Step 2 Open Device Manager.

Step 3 Select iSCSI from the IP menu. The iSCSI dialog is displayed.

Step 4 Select the Targets tab if it is not already selected.

Step 5 Click the Create button. The Create iSCSI Targets dialog is displayed. Use this dialog to map Fiber Channel LUNs to iSCSI LUNs:

Step 6 Enter the iSCSI LUN name in the Name field.

Step 7 Enter the iSCSI LUN, Port WWN, and FC LUN information in the appropriate fields.

Step 8 When finished, click Create to add this LUN to the table. Click Close to exit the Create iSCSI LUN Mappings dialog without adding the LUN.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Viewing iSCSI Statistics

To view iSCSI statistics, perform the following steps:

Step 1 Be sure you are connected to a switch that contains an IPS module.

Step 2 Open Device Manager.

Step 3 Select Statistics from the IP menu. The Statistics dialog is displayed.

Step 4 Select the iSCSI tab if it is not already selected.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Viewing iSCSI Sessions

To view iSCSI sessions, perform the following steps:

Step 1 Be sure you are connected to a switch that contains an IPS module.

Step 2 Open Device Manager.

Step 3 Select iSCSI from the IP menu. The iSCSI dialog is displayed.

Step 4 Select the Session Initiators tab if it is not already selected.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Viewing Session Statistics

To view session statistics, perform the following steps:

Step 1 Be sure you are connected to a switch that contains an IPS module.

Step 2 Open Device Manager.

Step 3 Select iSCSI from the IP menu. The iSCSI dialog is displayed.

Step 4 Select the Session Statistics tab if it is not already selected.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Creating an iSCSI Initiator

To create an iSCSI Initiator using Device Manager, follow these steps:

Step 1 Select iSCSI from the IP menu.

Step 2 Click the Initiators tab.

Step 3 Click the Create button.

The Create Initiators dialog is displayed.

Step 4 Enter the IP address, or the IQN name created from the iSCSI driver running on the initiator. The IQN name must be at least 16 characters.

Step 5 Assign names for the node WWN and port WWN fields.

There are three options. The **Auto** option assigns the WWN from a pool of about 440,000 WWNs per switch and is returned to pool when you log out. The **Persistent** option also assigns the WWN from a pool. However, when you log out of the switch, the WWIN is not returned to the pool but is saved for the initiator. The third option is to statically assign the WWN by manually entering WWN that the initiator will use.

Step 6 Select **Create** when all fields are complete, to create the initiator

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Creating an iSCSI Virtual Target

To create an iSCSI Initiator using Device Manager, follow these steps:

Step 1 Select iSCSI from the IP menu.

Step 2 Click the Targets tab.

Step 3 Click the Create button.

The Create Targets dialog is displayed.

Step 4 Enter the logical name to give to this virtual target.

Step 5 Click the drop-down button to the right of the pWWN field.

Step 6 Select the pWWN of the FC target that will be advertised as an iSCSI virtual target.

The drop-down list shows all pWWNs that are logged into the name server.

Step 7 Select the iSCSI initiators that will access this virtual target.

Select **All** if you want all the initiators to access the target. Select **None**, and then enter in the numbers by hand (separated by commas) if you want only certain initiators to access the target.

Step 8 Select **Create** when all fields are complete, to create the virtual target.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

CHAPTER 12

Managing IP Services

You can use Fabric Manager to configure IP filters and profiles. The general procedure is to create an IP profile, add a filter to the profile, and then associated that profile to one or more interfaces. Filters can only be created if their associated filter profiles already exist in the ProfileTable.

Deleting any profile in the Profile Table will also delete all the associated filters in the FilterTable and cause the state of the associated 'active' filter profile in the ProfileTable to be changed to 'notReady'.

Note In general, use the IP Wizard to manage IP filters. The procedures provided here are provided if you would prefer to manage IP filters manually.

The list below shows the IP Filter tasks you can perform with Fabric Manager. IP Filter is not available from Device Manager.

Using the IP Filter Wizard

You use the IP Filter Wizard to manage IP filters.

Step 1 From the Fabric Manager, choose **IP Filter** from the Fabric Manager **Edit** menu.

The **IP Filter Wizard** is displayed.

Step 2 Follow the prompts in the wizard to manage IP filters.

Creating IP Profiles

To create an IP profile, perform the following steps.

Step 1 From the Fabric Manager, choose **Security > IP Filter** from the menu tree.

The information pane of the Fabric Manager displays IP Filter information.

Step 2 Click the **Profiles** tab.

A list of profiles is displayed.

Step 3 Click the Create Row icon.

The Create Profile dialog box is displayed.

Step 4 Select the switches you want to include in the profile, by checking the checkboxes next to the switch's address.

Step 5 Enter a profile name in the Name field.

Step 6 Click the **Create** button to create the profile, or click the **Close** button to close the Create Profile dialog box without creating a profile.

The newly created profile is displayed in the list of profiles.

Step 7 To create additional profiles, repeat Step 6. Otherwise, click the **Close** button to close the Create Profile dialog box.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Adding IP Filters to Profiles

To add an IP filter to a profile, perform the following steps.

Step 1 From the Fabric Manager, choose **Security > IP Filter** from the menu tree.

The information pane of the Fabric Manager displays IP Filter information.

Step 2 Click the **Profiles** tab.

A list of switches and associated profiles is displayed.

Step 3 Click on the IP address of the switch to which you want to add a filter.

The Rules button becomes available.

Step 4 Click the **Rules** button.

The **IP Filter Edit** dialog box is displayed.

Step 5 Click the Create Row button.

The Create IP Filter dialog box is displayed.

Step 6 Complete the fields in the **Create IP Filter** dialog box.

Step 7 Click the **Create** button to create the filter, or click the **Close** button to close the Create IP Filter dialog box without creating a filter.

The newly created filter is displayed in the list of filters.

Step 8 Repeat Step 7 to create additional filters, or click the **Close** button to close the Create IP Filter dialog box.

Step 9 Click the Apply Changes button to add the newly created filters to the profile.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Associating IP Profiles to Interfaces

To associate the profile to an interface, perform the following steps.

Step 1 From the Fabric Manager, choose **Security** > **IP Filter** from the menu tree.

The information pane of the Fabric Manager displays IP Filter information.

Step 2 Click the **Interfaces** tab.

A list of interfaces and associated profiles is displayed.

Step 3 Click the Create Row icon.

The Create Interface dialog box is displayed.

Step 4 Select the switches you want to include in the profile, by checking the checkboxes next to the switch's address.

Step 5 Enter an interface name in the Name field.

Step 6 Select the profile direction (either inbound or outbound).

Step 7 Enter the profile name in the Profile Name field. (Note, this profile name must already have been created using the Create Profiles dialog. If not, no filters will be enabled until you to go to the Create Profiles dialog and create the profile.

Step 8 Click the **Create** button to associate the profile, or click the **Close** button to close the Create Interfaces dialog box without associating a profile.

The newly associated profile is displayed in the list of profiles.

Step 9 Repeat Step 8 to create additional associations, or click the **Close** button to close the Create Interfaces dialog box.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Deleting IP Profiles

To delete an IP profile, perform the following steps.

Step 1 From the Fabric Manager, choose **Security > IP Filter** from the menu tree.

The information pane of the Fabric Manager displays IP Filter information.

Step 2 Click the **Profiles** tab.

A list of switches, profile names, and profile types is displayed.

Step 3 Select the row you want to delete. If you want to delete multiple rows, hold down the Shift key while selecting rows.

Step 4 Click the Delete Row icon.

The profiles are deleted.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Deleting IP Filters

To delete an IP filter, perform the following steps.

Step 1 From the Fabric Manager, choose **Security > IP Filter** from the menu tree.

The information pane of the Fabric Manager displays IP Filter information.

Step 2 Click the **Interfaces** tab.

A list of switches, filters, and profile names is displayed.

Step 3 Select the row you want to delete. If you want to delete multiple rows, hold down the Shift key while selecting rows.

Step 4 Click the Delete Row icon.

The filters are deleted from the profile.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

CHAPTER 13

Managing FICON

FI-bre CON-nection (FICON) interface capabilities enhances the Cisco MDS 9000 Family by supporting both open systems and mainframe storage network environments. Inclusion of Control Unit Port (CUP) support further enhances the MDS offering by allowing inband management of the switch from FICON processors.

Note The FICON feature is managed exclusively through Device Manager.

For details on FICON and the CLI-specific support of FICON, refer to the *Cisco MDS 9000 Family Configuration Guide*.

This chapter includes the following sections:

FICON Procedures

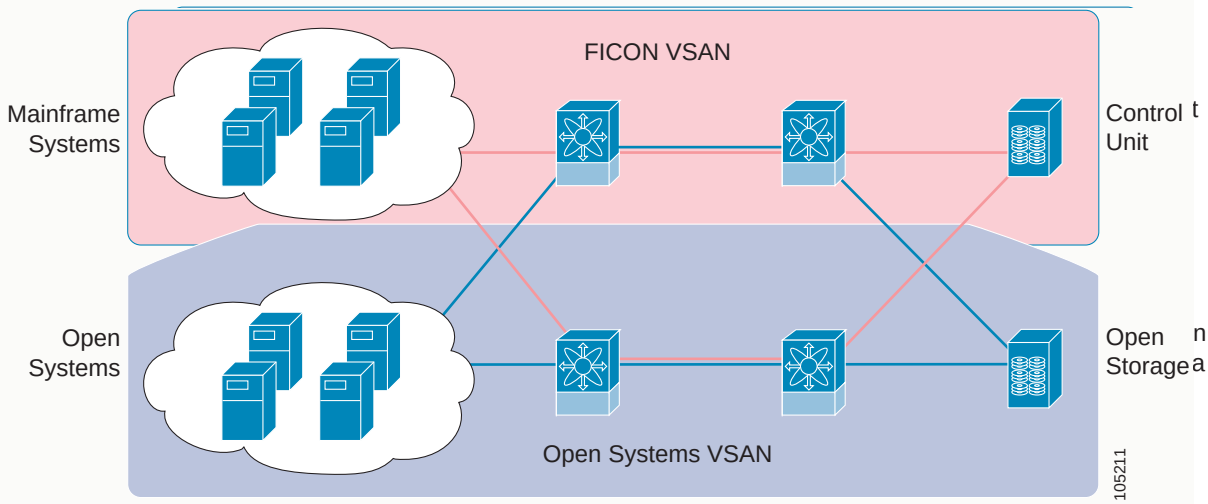
The following procedures can be performed for FICON using Device Manager:

Note FICON features can be implemented in any switch in the Cisco MDS 9000 Family running SAN-OS Release 1.3(x) or above. No hardware changes are required to configure FICON parameters.

About FICON

The Cisco MDS 9000 Family supports Fibre Channel protocol (FCP), FICON, iSCSI, and FCIP capabilities within a single, high availability platform. This solution simplifies purchasing, reduces deployment and management costs, and reduces the complex evolution to shared mainframe and open systems storage networksFigure 13-1.

Figure 13-1 Shared System Storage Network



FCP and FICON are different FC4 protocols and their traffic are independent of each other. If required, devices using this protocol can be isolated using VSAN-based zoning.

MDS-Specific FICON Advantages

The following advantages enhance an already effective network by using FICON:

- Fabric-Optimization with VSANs, page 13-3
- FCIP Support, page 13-4
- PortChannel Support, page 13-5
- VSANs for FICON and FCP Intermixing, page 13-5
- MDS-Supported FICON Features, page 13-5

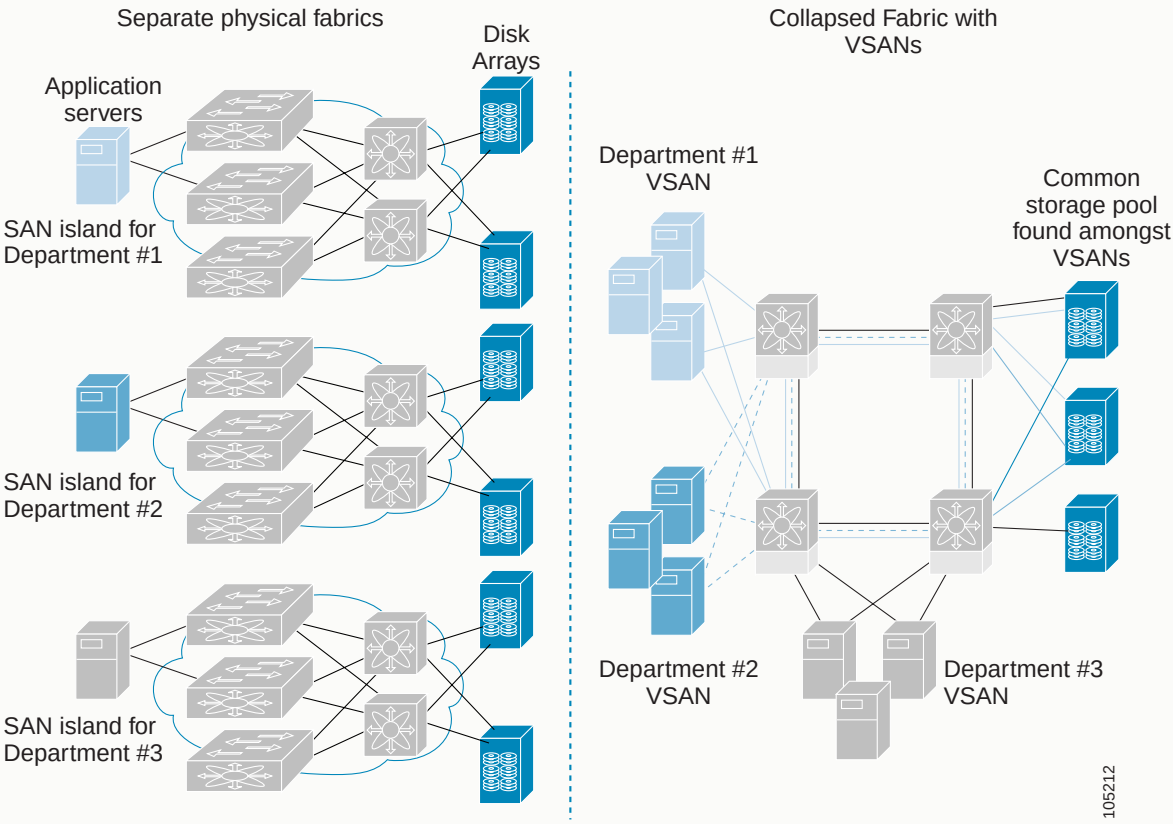
Fabric-Optimization with VSANs

Generally, separate physical fabrics have a high level of switch management and have a higher implementation cost. Further, the ports in each island may be over-provisioned depending on the fabric configuration.

By using the Cisco MDS-specific VSAN technology, you can introduce greater efficiency between these physical fabric by lowering the cost of over-provisioning and reducing the number of switches to be managed.

VSANs also help you to move unused ports nondisruptively and provides a common redundant physical infrastructure.Figure 13-1

Figure 13-2 VSAN-specific Fabric Optimization



VSANs enable global SAN consolidation by allowing you to convert existing SAN islands into virtual SAN islands on a single physical network. It provides hardware-enforced security and separation between applications or departments to allow coexistence on a single network. It also allows virtual rewiring to consolidate your storage infrastructure. You can move assets between departments or applications without the expense and disruption of physical relocation of equipment.

FCIP Support

The multilayer architecture of the Cisco MDS 9000 Family enables a consistent feature set over a protocol-agnostic switch fabric. Cisco MDS 9500 Series and MDS 9216 switches transparently integrate Fibre Channel, FICON and Fibre Channel over IP (FCIP) in one system. The FICON over FCIP feature enables cost-effective access to remotely located mainframe resources. With the MDS 9000 platform, storage replication services such as IBM PPRC and XRC can be extended over metro to global distances using ubiquitous IP infrastructure and simplifying business continuance strategies.

The Cisco MDS implementation of FICON provides support for IP tunneling to efficiently consolidate SANs over WAN distances. IP tunnels enable a globally accessible storage infrastructure.

PortChannel Support

The Cisco MDS implementation of FICON provides support for efficient utilization and increased availability of inter-switch links necessary to build stable large-scale SAN environments. PortChannels ensure an enhanced ISL availability and performance is Cisco MDS switches.

VSANs for FICON and FCP Intermixing

Cisco MDS 9000 Family FICON-enabled switches simplify deployment of even the most complex intermix environments. Multiple logical FICON, Z-Series Linux/FCP and Open-Systems FCP fabrics can be overlaid onto a single physical fabric by simply creating VSANs as required for each service. VSANs provide both hardware isolation and protocol specific fabric services, eliminating the complexity and potential instability of zone-based intermix schemes.

By default, the FICON feature is disabled in all switches in the Cisco MDS 9000 Family. When the FICON feature is disabled, FC IDs can be allocated seamlessly. Intermixed environments are addressed by the SAN-OS software. The challenge of mixing Fibre Channel Protocol (FCP) and FICON protocols are addressed by Cisco MDS switches when implementing VSANs.

Switches and Directors in the Cisco MDS 9000 Family support FCP and FICON protocol intermixing at the port level. If these protocol are intermixed in the same switch, you can use VSANs to isolate FCP and FICON ports. When creating an intermix environment, place all FICON devices in one VSAN (other than the default VSAN) and segregate the FCP switch ports in a separate VSAN (other than the default VSAN). This isolation ensures proper communication for all connected devices.

MDS-Supported FICON Features

The Cisco MDS 9000 Family FICON features include:

- Flexibility and investment protection—The Cisco MDS 9000 Family shares common switching and service modules across all Cisco MDS 9500 Series as well as the Cisco MDS 9216 Switch. (refer to the *Cisco MDS 9500Series* and the *Cisco MDS 9216 Switch Hardware Installation Guides).*
- High-availability FICON-enabled director—The Cisco MDS 9500 Series combines nondisruptive software upgrades, stateful process restart and failover, and full redundancy of all major components for a new standard in director-class availability. It supports up to 224 2/1-Gbps, autosensing FICON or Fibre Channel FCP ports in any combination in a single chassis and up to 768 Fibre Channel ports in a single rack—1.44 Tbps of internal system bandwidth ensures smooth integration of future 10-Gbps modules.
- Infrastructure protection—Common software releases infrastructure protection is available across all Cisco MDS 9000 platforms.
- VSAN technology—The Cisco MDS 9000 Family introduces VSAN technology for hardware-enforced, isolated environments within a single physical fabric for secure sharing of physical infrastructure and enhanced FICON intermix support.
- Port-level configurations:
  - BB_credits for each port.
  - Port security for each port.
  - Enable beaconing for ports and the director unit.
- Configure an alias name, instead of the WWN, for switches and attached node devices.

- Comprehensive security framework—The Cisco MDS 9000 Family supports RADIUS authentication, Simple Network Management Protocol Version 3 (SNMPv3), role-based access control, Secure Shell Protocol (SSH), Secure File Transfer Protocol (SFTP), Fibre Channel Security Protocol (FC-SP), VSANs, hardware-enforced zoning, LUN zoning, read-only zones, ACLs, port security, fabric binding and VSAN-based access control.
- View the local accounting log to locate FICON events and timestamps.
- Unified storage management—Cisco MDS 9000 FICON-enabled switches are fully IBM CUP standard compliant for in-band management using the IBM S/A OS/390 I/O operations console.
- Port address-based configurations—port name, blocked or unblocked state, and the prohibited connection attributes.
- Display the following information:
  - Individual Fibre Channel ports, such as the port name, port number, Fibre Channel address, operational state, type of port, and login data.
  - Nodes attached to ports.
  - Port performance and statistics.
- Store and apply configuration files (see the "FICON Configuration Files" section on page 13-12).
- FICON and Open Systems Management Server features if installed (see the "VSANs for FICON and FCP Intermixing" section on page 13-5).
- Enhanced Cascading Support.
- Set the date and time on the switch.
- Configure SNMP trap recipients and community names.
- Call Home configurations—director name, location, description, and contact person.
- Configure preferred domain ID, FC ID persistence, and principle switch priority.
- Sophisticated SPAN diagnostics—The Cisco MDS 9000 Family provides industry-first intelligent diagnostics, protocol, decoding, and network analysis tools as well as integrated call-home capability for added reliability, faster problem resolution, and reduced service costs .
- Configure R_A_TOV, E_D_TOV.
- Perform maintenance tasks for the director including maintaining firmware levels, accessing the director logs, and collecting data to support failure analysis.
- Clear port-level incident alerts.

FICON Terminology

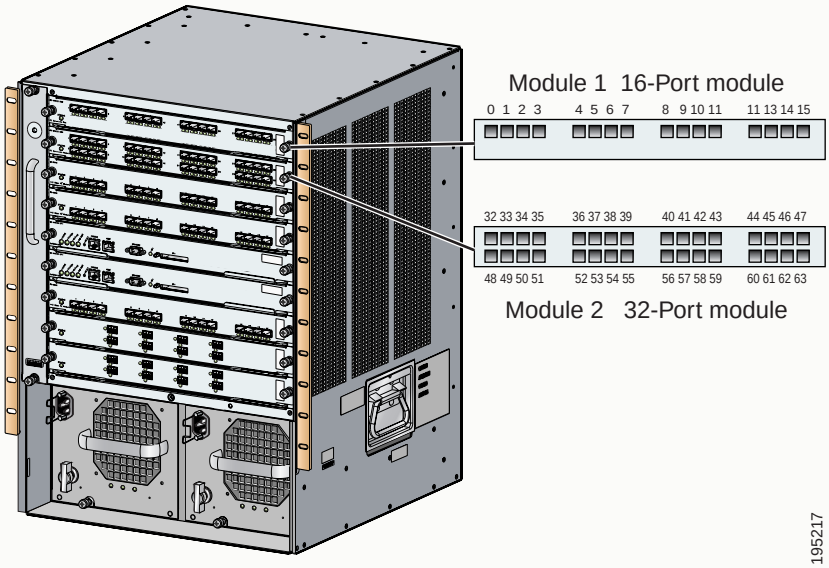
This section explains the basic FICON terms used in this chapter.

- *Channel*—A channel is an entity that is typically mapped to an N-port in a host computer. The host computer accesses I/O devices. Multiple, concurrent I/O devices can connect to a single FICON channel. A Channel is equivalent to a SCSI initiator.
- *Channel Image*—A channel image represents a separate logical channel. Each N-port can have multiple channel images.
- *Control Unit*—A control unit is the interface to the I/O device. Each control unit can be responsible for multiple devices at the same time. A control unit is equivalent to a SCSI target. It is attached to the fabric by one or more N-ports.
- *Control Unit Image*—Each control unit can have multiple control unit images.
- *Channel-to-Channel*—Channel-to-channel (CTC) communication provides interconnection from one server to another.

FICON Port Numbering

With reference to the FICON feature, ports in Cisco MDS switches are identified by a statically defined 8-bit value known as the *port number*. Port numbers are assigned based on the module and the slot in the chassis. Port numbers cannot be changed and the first port in a switch always starts with a 0 (see Figure 13-3).

Figure 13-3 Port Number in the Cisco MDS 9000 Family



The FICON port number is assigned based on the front panel location of the port and is specific to the slot in which the module resides. Even if the module is a 16-port module, 32-port numbers are assigned to that module—regardless of the module type (16-port or 32-port), the module's physical presence in the chassis, or the port status (preset or not preset).

Note Only Fibre Channel, PortChannel, and FCIP ports are mapped to FICON port numbers. Other types of interfaces do not have a corresponding port number.

Table 13-1 lists the port number assignment for the Cisco MDS 9000 Family of switches and directors.

Table 13-1 FICON Port Numbering in the Cisco MDS 9000 Family

Product	Slot Number	Implemented Port Numbers Allocation		Unimplemented Port Number s	Notes
		To Ports	To PortChannels		
Cisco MDS 9120 Switch	Not applicable	Ports 0 through 39	40 through 55	Ports 56 through 253 and Port 255	Only 20 ports are used.
Cisco MDS 9140 Switch	Not applicable	Ports 0 through 39	40 through 55	Ports 56 through 253 and Port 255	All 40 ports are used.
Cisco MDS 9216 Switch	Slot 1	Ports 0 through 31	64 through 79	Ports 80 through 253 and Port 255	Similar to a switching module
	Slot 2	Ports 32 through 63			The first 16 port numbers in a 16-port module are used and the rest remain unused.
Cisco MDS 9506 Director	Slot 1	Ports 0 through 31	Ports 128 through 143	Ports 144 through 253 and Port 255	
	Slot 2	Ports 32 through 63			
	Slot 3	Ports 64 through 95			
	Slot 4	Ports 96 through 127			
	Slot 5	None			Supervisor module are not allocated port numbers.
	Slot 6	None			
Cisco MDS 9509 Director	Slot 1	Ports 0 through 31	Ports 224 through 239	Ports 240 through 253 and Port 255	The first 16 port numbers in a 16-port module are used and the rest remain unused.
	Slot 2	Ports 32 through 63			
	Slot 3	Ports 64 through 95			
	Slot 4	Ports 96 through 127			
	Slot 5	None			Supervisor module are not allocated port numbers.
	Slot 6	None			
	Slot 7	Ports 128 through 159			The first 16 port numbers in a 16-port module are used and the rest remain unused.
	Slot 8	Ports 160 through 191			
	Slot 9	Ports 192 through 223			

Implemented and Unimplemented Ports

An implemented port refers to any port number that is available in the chassis. These numbers are identified in the Implemented Port Numbers Allocation column in Table 13-1.

An unimplemented port refers to any port number that is not available in the chassis. These numbers are identified in the Unimplemented Port Number s column in Table 13-1.

Tip An unimplemented port is prohibited from communicating with an implemented port in a FICON setup and cannot be configured.

Installed and Uninstalled Ports

An installed port refers to a port for which all required hardware is present. A specified port number in a VSAN can be implemented, and yet not installed if any of the following conditions apply:

- The module is not present.
- The small form-factor pluggable (SFP) port is not present.
- The port is not in a FICON-enabled VSAN.
- The port is part of a PortChannel number allocation.

For example:

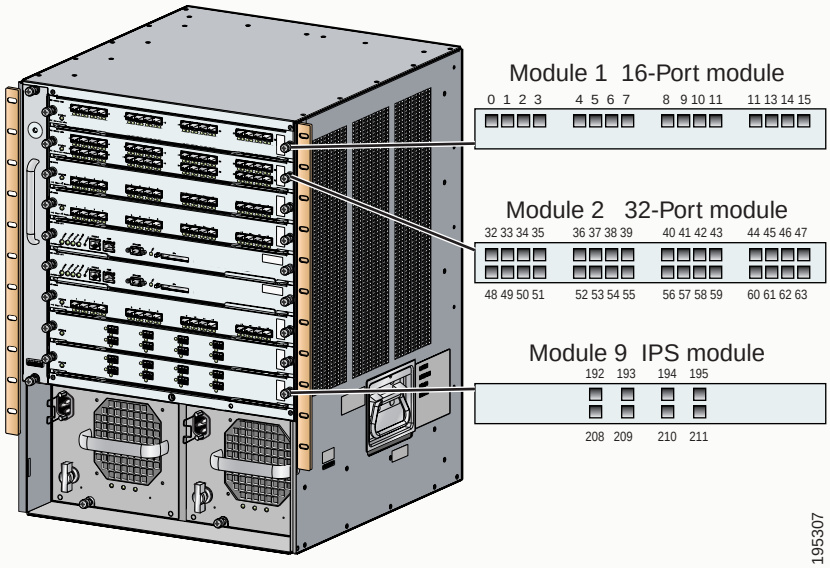
- If module 1 is not physically present in slot 1 in a Cisco MDS 9509 Director, port numbers 0 to 31 are considered uninstalled.
- If a 16-port module is inserted in slot 2 in a Cisco MDS 9509 Director, port numbers 38 to 63 are considered uninstalled.
- If port number 4 (of a 16-port module in slot 1) is configured in FICON-enabled VSAN 2, then only port 4 is installed and ports 0 to 3 and 5 to 15 are uninstalled—even if they are implemented.
- If interface fc1/1 (port address = 0) is a TE port and is configured in VSANs 1 through 20—but only VSANs 2 and 3 are FICON-enabled, then port address 0 is only installed in VSAN 2 and VSAN 3.

FCIP Port Number

You must explicitly configure FCIP port numbers. The port address for FCIP ports are configured to the range of numbers that you can use are restricted to the port numbers available in the IPS modules slot. If an IPS module is in Slot 9 in a Cisco MDS 9509 Director, the available range of port numbers is 192 through 223. The FCIP interface can be assigned any port number that is available within that range.

For example, if the FCIP port is bound to GigabitEthernet interface 9/1, the assigned FCIP port numbers can be 192, 193, 194, 195, 208, 209, 210, and 211Figure 13-3.

Figure 13-4 FCIP Port Number s in the Cisco MDS 9000 Family



Note Gigabit Ethernet ports do not have a corresponding mapping to the FICON port number concept.

Use the **show fcip portnumber** command to view the list of available port numbers for a specified module.

Port Numbering Summary

The following guidelines apply to FICON port numbers:

- Supervisor modules do not have port number assignments.
- Port number are VSAN independent—Fibre Channel port numbers do not change based on VSANs or TE ports.
- Each PortChannel must be explicitly associated with a FICON port number.
- Physical ports in a PortChannel become uninstalled. These port number are not applied in the FICON configurations, but the PortChannel configuration is applied to the physical ports.
- A FCIP tunnel must be explicitly associated with a FICON port number—If the port number is not assigned for PortChannels or for FCIP tunnels, the associated ports will not come up (see the "FCIP Port Number" section on page 13-9).
- iSCSI and virtualization ports are not exposed to FICON and do not have FICON port number associations.

Port Addresses

By default, port numbers are the same as port addresses. The default port address changes when you issue the port swap command at any time. When you issue this command, the port addresses are swapped (see the "Swapping FICON Ports" section on page 13-16).

FC ID Allocation

FICON requires a predictable and static FC ID allocation scheme. When FICON is enabled, the FC ID allocated to a device is based on the port address of the port to which it is attached. The port address forms the middle byte of the fabric address. Additionally, the last byte of teh fabric address should be the same for all devices in the fabric. By default, the last byte valud is 0 and can be configured.

Cisco MDS switches have a dynamic FC ID allocation scheme. When FICON is enabled or disabled on a VSAN, all the ports are flapped to switch between the dynamic and static FC IDs and vice versa.

Note You cannot configure persistent FC IDs in FICON-enabled VSANs.

MDS FICON Prerequisites

By default, the FICON feature is disabled. To enable FICON (ensure that a FICON VSAN can be operationally up), all of the following requirements must be met:

- Set the default zone to permit, if you are not using the zoning feature.
- Enable in-order delivery on the switch.
- Enable (and if required, configure) fabric binding on the VSAN.
- Verify that the configured domain ID and requested domain ID match.
- Verify that conflicting persistent FCIDs do not exist in the switch.
- Add the CUP (ara FE) to the zone, if you are using zoning.

If any of these requirements are not met, the FICON feature cannot be enabled.

Note The process of creating a FICON VSAN will automatically perform the above steps.

FICON Configuration Files

You can save up to 16 FICON configuration files on each FICON-enabled VSAN (in persistent storage). The file format is proprietary to IBM™. These files can be read and written by IBM hosts using the inband CUP protocol. Additionally, you can use the Cisco MDS CLI or FM applications to operate these FICON configuration files

Note Multiple FICON configuration files with the same name can exist in the same switch, provide they reside in different VSANs. For example, you can create a configuration file named XYZ in both VSAN 1 and VSAN 3.

When you enable the FICON feature in a VSAN, the switches always uses the startup FICON configuration file, called IPL. This file is created with a default configuration as soon as FICON is enabled on a VSAN.

FICON configuration files contain the following configuration for each implemented port address:

- Host control
- Block
- Prohibit mask
- Port address name

Note Refer to "Working with Configuration Files" in the *Cisco MDS 9000 Family Configuration Guide* for details on the normal configuration files used by Cisco MDS switches. This configuration file includes FICON enabled attribute for a VSAN, port number mapping for port channels and FCIP interfaces, port number to port address mapping ("Swapping FICON Ports" section on page 13-16), port and trunk allowed VSAN configuration for ports, in-order guarantee, configuring static (insistent) domain ID, and fabric binding configuration.

Writing to the IPL file

When configuring FICON you will predominantly be working with FICON-related configurations. The non-FICON configurations are used to initially configure the switch. You can save FICON configuration files using two methods: snapshot of running configuration or automatically saving the running configuration.

Caution When FICON is disabled on a VSAN, all the FICON configuration files are irretrievably lost.

Accessing FICON Configuration Files

Only one user can access the configuration file at any given time:

- While this file is being accessed by user 1, user 2 cannot access this file.
- When user 2 does attempt to access this file, an error is issued to user 2.
- If user 1 has been inactive for more than 15 seconds, the file is automatically closed and available for use by any other permitted user.

FICON configuration files can be accessed by any host SNMP CLI user who is permitted to access the switch. The locking mechanism in the SAN-OS software restricts access to one user at a time per file. This lock applies to newly-created files and previously-saved files. Before accessing any file, you must lock the file and obtain the file key. A new file key is used by the locking mechanism for each lock request. The key is discarded when the lock timeout of 15 seconds expires. The lock timeout value cannot be changed.

Creating FICON VSANs (enabling FICON)

The VSAN that is created here does not need to be a new VSAN. It is a new FICON VSAN. When a new FICON VSAN is created, static (insistent) domain IDs, in-order delivery, and fabric binding must be enabled so the FICON VSAN can operate. When you enable the FICON feature in Cisco MDS switches, the following apply:

- The IPL configuration file is automatically created (see the "FICON Configuration Files" section on page 13-12).
- You cannot disable in-order delivery, fabric binding, or static(insistent) domain ID configurations.

If you specify an existing VSAN with operational traffic to be used for the FICON VSAN, the traffic will be disrupted. In this case, a warning message is displayed before you create the FICON VSAN.

To create a FICON VSAN, perform this procedure:

Step 1 From Device Manager, select VSANs from the FICON menu.

The FICON VSANs/Files configuration dialog is displayed.

Step 2 Ensure that the VSANs tab is enabled.

Step 3 Click the Create button

The Create FICON VSANs dialog is displayed.

Step 4 Enter the VSAN ID.

Step 5 Enter the Domain ID.

Step 6 Click Create to create the new VSAN, or click Close to close the dialog without creating the VSAN.

Entering FICON Port Configuration Information

To display FICON Port Configuration information, perform this procedure:

Step 1 From Device Manager, select VSANs from the FICON menu.

The FICON VSAN configuration dialog is displayed.

Step 2 Ensure that the VSANs tab is enabled.

Step 3 Click anywhere in the row for the VSAN for which you want to configure port information.

Step 4 Click the Port Configuration button to display the Port Configuration dialog.

Step 5 Enter the Port Configuration information. Click Apply to save the configuration information, or click Cancel to exit the dialog without saving.

Viewing FICON Port Attributes

To view FICON port attributes, perform this procedure:

Step 1 From Device Manager, select VSANs from the FICON menu.

The FICON VSAN configuration dialog is displayed.

Step 2 Ensure that the VSANs tab is enabled.

Step 3 Click anywhere in the row for the VSAN for which you want to configure port information.

Step 4 Click the Port Attributes button to display the Port Attributes dialog.

Viewing FICON Director History

To view FICON director history, perform this procedure:

Step 1 From Device Manager, select VSANs from the FICON menu.

The FICON VSAN configuration dialog is displayed.

Step 2 Ensure that the VSANs tab is enabled.

Step 3 Click anywhere in the row for the VSAN for which you want to configure port information.

Step 4 Click the Director History button to display a history of FICON-related changes to this switch.

Deleting FICON VSANs (Disabling FICON)

To delete a FICON VSAN, perform this procedure:

Step 1 From Device Manager, select VSANs from the FICON menu.

The FICON VSAN configuration dialog is displayed.

Step 2 Ensure that the VSANs tab is enabled.

Step 3 Click anywhere in the row for the VSAN for which you want to configure port information.

Step 4 Click the Delete button to delete the VSAN.

Note Deleting the VSAN will also delete the associated FICON configuration file, and the file cannot be recovered.

Creating FICON Files

If a specified file does not exist, it is created. Up to 16 files can be saved. Each file name is restricted to 8 alphanumeric characters. To create a FICON file, perform this procedure:

Step 1 From Device Manager, select VSANS from the FICON menu.

The FICON VSANs/Files dialog is displayed.

Step 2 Click the Files tab.

Step 3 Click the Create button

The Create FICON VSANs Files dialog is displayed.

Step 4 Enter the VSAN ID.

Step 5 Enter the File Name.

Step 6 Enter the Description.

Step 7 Click Create to create the new file, or click Close to close the dialog without creating the file.

Deleting FICON Files

To delete a FICON file, perform this procedure:

Step 1 From Device Manager, select VSANS from the FICON menu.

The FICON VSANs/Files dialog is displayed.

Step 2 Click the Files tab.

Step 3 Click anywhere in the row for the file you want to delete.

Step 4 Click the Delete button to delete the file.

Copying FICON Files

The SAN-OS software maintains different configuration files to support a FICON network. These configuration files can be are saved using the **copy running-config startup-config** command, or using Device Manager. FICON configuration files do not contain the following information that is normally saved with the running configuration:

- Port number to port address mapping
- PortChannel to port number mapping
- Port swap occurrences
- FICON enabled VSANs

FICON configuration files are independent of these parameters. Instead, this information is stored in persistent storage as they can be modified independent of the startup configuration.

To copy a FICON file, perform this procedure:

Step 1 From Device Manager, select VSANs from the FICON menu.

The FICON VSANs/Files dialog is displayed.

Step 2 Click the Files tab.

Step 3 Click to highlight the row for the file you want to copy.

Swapping FICON Ports

The port swap FICON feature is only provided for maintenance purposes and is supported in all switches in the Cisco MDS 9000 Family support this feature.

MDS switches also allow port swapping for non-existent ports as specified below:

- Only FICON-specific configurations (port number to port address mapping) is swapped
- No other system configuration is swapped.
- All other system configurations are only maintained for existing ports.

Once you swap ports, the switch automatically performs the following actions:

- Shuts down both the old and new ports
- Swaps the port configuration
- Initializes the port shut down.

If a physical Fibre Channel port must be swapped with another Fibre Channel port that is not being used, you can swap the port configuration.

Port Swapping Guidelines

Be sure to follow these guidelines when using the FICON port swap feature:

- Port swapping is not supported for logical ports (PortChannels, FCIP links). Neither the *old-port-number* nor the *new-port-number* can be a logical port.
- Port swapping is not supported between physical ports that are part of a PortChannel. Neither the *old-port-number* nor the *new-port-number* can be a physical port that is part of a PortChannel.
- Before performing a port swap, the SAN-OS software performs a compatibility check. If the two ports have incompatible configuration, the port swap is rejected with an appropriate reason code. For example, if a port with BB_credits as 25 is being swapped with an OSM port for which a maximum of 12 BB_credits is allowed (not a configurable parameter), the port swap operation is rejected.
- If ports have default values (for some incompatible parameters), then port swap is allowed to go through and the ports retain their default values.

Note The 32-port module guidelines also apply for port swapping configurations (refer to the *Cisco MDS 9000 Family Configuration Guide* for more information).

Port Swapping Procedure

To swap ports:

Step 1 Select two Fibre Channel ports, by holding down the CTRL key and clicking on them with the mouse.

Step 2 Select **Swap Selected Ports** from the FICON menu.

Configuring Code Pages

FICON strings are coded in Extended Binary-Coded Decimal Interchange Code (EBCDIC) format. Use the **code-page** command to configure the EBCDIC format. Refer to your mainframe documentation for details on the code page options. Cisco MDS switches support **international-5**, **france**, **brazil**, **germany**, **italy**, **japan**, **spain-latinamerica**, **uk**, and **us-canada** (default) EBCDIC format options.

Tip This is an optional configuration. If you are not sure of the EBCDIC format to be used, we reccommend retaining the **us-canada** (default) option.

Configuring Fabric Binding

The SAN-OS 1.3(x) fabric binding feature ensures ISLs are only enabled between specified switches in the fabric binding configuration. Fabric binding is configured on a per-VSAN basis, and can only be implemented in FICON VSANs. You can still perform fabric binding configuration in a non-FICON VSAN—these configurations will only come into effect after FICON is enabled. This feature helps prevent unauthorized switches from joining the fabric or disrupting current fabric operations. It uses the Exchange Fabric Membership Data (EFMD) protocol in FICON networks to ensure an persistent domain ID for switches.

The fabric binding feature must be enabled in each switch in the fabric that participate in the fabric binding. By default, this feature is disabled in all switches in the Cisco MDS 9000 Family. The configuration and verification commands for the fabric binding feature are only available when fabric binding is enabled on a switch. When you disable this configuration, all related configurations are automatically discarded.

The fabric binding maintains a configuration database (config-database) and an active database. The config-database is a read-write database which collects the configurations you perform. These configurations are only enforced upon activation. This activation overwrites the active database with the contents of the config-database. The active database is read-only and is the database that checks each switch that attempts to login.

By default, the fabric binding feature is not activated. You cannot activate the switch if one of the following situations apply to your configuration:

- The configured database is empty.
- Missing or conflicting entries exist in the configured database as compared to the active database.

If the database activation is rejected due to one or more conflicts listed in the previous section, you may decide to proceed with the activation by using the **force** option.

Note **Note** An activation using the **force** option does not log out existing devices even if they violate the active database.

Port Security versus Fabric Binding

Port security and fabric binding are two independent features that can be configured to complement each other (see Table 13-2).

Table 13-2 Fabric Binding and Port Security Comparison

Fabric Binding	Port Security
Configured using a set of sWWN and a persistent Domain ID.	Configured using pWWNs/nWWNs or fWWNs/switch WWNs.
Binds the fabric at the switch level.	Binds devices at the interface level.

Table 13-2 Fabric Binding and Port Security Comparison

Fabric Binding	Port Security
Only the configured sWWN stored in the fabric binding database will be authorized to participate in the fabric.	Allows a preconfigured set of Fibre Channel devices to logically connect to a SAN port(s). The switchport, identified by a WWN or interface number, connects to a Fibre Channel device (a host or another switch), also identified by a WWN. By Binding these two devices, you lock these two ports into a group (list).
Activation is required on a per VSAN basis.	Activation is required on a per VSAN basis.
User defines specific switches which are allowed to connect to the fabric, regardless of the physical port to which the peer switch is connected.	User specifies the specific physical port(s) to which another device can connect
Does not learn logging in switches.	Learns about switches/devices if in learning mode.

Port-level Checking for xE ports

- Switch login—uses both Port Binding as well as the Fabric Binding feature for a given VSAN.
- Binding checks are done on the port VSAN:
  - E-port security binding check done on port VSAN.
  - TE-port security bindings check done in each vsan allowed.

While port security complements fabric binding, they are independent features and can be enabled or disabled separately.

Activating Fabric Binding

The fabric binding feature must be enabled in each switch in the fabric that participate in the fabric binding. By default, this feature is disabled in all switches in the Cisco MDS 9000 Family.

To activate fabric binding, follow these steps:

Step 1 From Device Manager, select Fabric Binding from the FICON menu.

The Fabric Binding dialog is displayed.

Step 2 Ensure that the Actions tab is enabled.

Step 3 Click in the Actions column for the VSAN(s) for which you want to activate fabric binding.

Step 4 Select Activate or Force Activate.

Step 5 Click Apply to activate the fabric binding, or click Close to close the dialog without activating fabric binding for the selected VSAN(s).

Configuring a List of sWWNs

A user-specified fabric binding list contains a list of switch WWNs (sWWNs) within a fabric. If a sWWN attempts to join the fabric, and that sWWN is not in the list or the sWWN is using a domain ID that differs from the one specified in the allowed list, the ISL between the switch and the fabric is automatically isolated in that VSAN and the switch is denied entry into the fabric.

The persistent domain ID must be specified along with the sWWN. Domain ID authorization is required in FICON VSANs where the domains are statically configured and the end devices reject a domain ID change in all switches in the fabric.

Deactivating Fabric Binding

To deactivate fabric binding, follow these steps:

Step 1 From Device Manager, select Fabric Binding from the FICON menu.

The Fabric Binding dialog is displayed.

Step 2 Ensure that the Actions tab is enabled.

Step 3 Click in the Actions column for the VSAN(s) for which you want to activate fabric binding.

Step 4 Select Deactivate.

Step 5 Click Apply to deactivate the fabric binding, or click Close to close the dialog without deactivating fabric binding for the selected VSAN(s).

Fabric Binding CopyActive to Config

To copy the active fabric binding to the configuration file, follow these steps:

Step 1 From Device Manager, select Fabric Binding from the FICON menu.

The Fabric Binding dialog is displayed.

Step 2 Ensure that the Actions tab is enabled.

Step 3 Click in the CopyActive ToConfig column for the VSAN(s) for which you want to copy fabric binding.

Step 4 Click Apply to copy the fabric binding, or click Close to close the dialog without copying the fabric binding for the selected VSAN(s).

Creating a Fabric Binding Configuration

To create a fabric binding configuration, perform this procedure:

Step 1 From Device Manager, select Fabric Binding from the FICON menu.

The Fabric Binding dialog is displayed.

Step 2 Click the Config Database tab.

Step 3 Click Create to display the Create Fabric Binding Config Database dialog.

Step 4 Enter the VSAN ID, the Peer WWN, and the Domain ID.

Step 5 Click Create to create the fabric binding configuration, or click Close to close the dialog without creating the fabric binding configuration.

Deleting a Fabric Binding Configuration

To delete a fabric binding configuration, perform this procedure:

Step 1 From Device Manager, select Fabric Binding from the FICON menu.

The Fabric Binding dialog is displayed.

Step 2 Click the Config Database tab.

Step 3 Click in the row for the VSAN for which you want to delete the fabric binding configuration.

Step 4 Click Delete to delete the fabric binding configuration, or click Close to close the dialog without deleting the fabric binding configuration.

Viewing Fabric Binding Active Database

To view the fabric binding active database, perform this procedure:

Step 1 From Device Manager, select Fabric Binding from the FICON menu.

The Fabric Binding dialog is displayed.

Step 2 Click the Active Database tab.

The active database is displayed.

Viewing Fabric Binding Violations

To view fabric binding violations, perform this procedure:

Step 1 From Device Manager, select Fabric Binding from the FICON menu.

The Fabric Binding dialog is displayed.

Step 2 Click the Violations tab.

The Violations are displayed.

Clearing Fabric Binding Statistics

To clear fabric binding statistics, perform this procedure:

Step 1 From Device Manager, select Fabric Binding from the FICON menu.

The Fabric Binding dialog is displayed.

Step 2 Click the Statistics tab.

The statistics are displayed.

Step 3 Check the checkbox in the Clear column for the VSAN(s) for which you want to clear statistics.

Step 4 Click the Apply button.

Viewing EFMD Statistics

To view EFMD statistics, perform this procedure:

Step 1 From Device Manager, select Fabric Binding from the FICON menu.

The Fabric Binding dialog is displayed.

Step 2 Click the EFMD Statistics tab.

The EFMD statistics are displayed.

Displaying RLIR Information

The Registered Link Incident Report (RLIR) application provides a method for a switchport to send a LIR to a registered Nx-port.

When a Link Incident Record (LIR) is detected in FICON-enabled switches in the Cisco MDS 9000 Family form a RLIR Extended Link Service (ELS) and sends it to the members in it's Established Registration List (ERL).

In case of multi-switch topology, a Distribute Registered Link Incident Record (DRLIR) Inter Link Service (ILS) are sent to all reachable remote domains along with the RLIR ELS. On receiving the DRLIR ILS, the switch extracts the RLIR ILS and sends to the members of the ERL.

The Nx-ports interested in receiving the RLIR ELS send Link Incident Record Registration (LIRR) ELS request to the management server on the Switch. The RLIRs are processed on a per-VSAN basis.

Note If an *always receive* RLIR is not registered for any N-port or if the delivery of an RLIR fails for one of those ports, then the RLIR is sent to a port registered to *conditional receive* RLIRs.

CHAPTER 14

Troubleshooting the Fabric

There are several things you can do to use Fabric Manager to troubleshoot your fabric.

Analyzing Switch Device Health

The Switch Health option lets you determine the status of the components of a specific switch. To use the Switch Health option, follow these steps:

Step 1 Click **Switch Health** from the Fabric Manager Tools menu.

The Switch Health Analysis window is displayed.

Step 2 Click **Start** to identify any problems that may currently be affecting the selected switch.

The Switch Health Analysis window displays any problems affecting the selected switches.

Step 3 Fix these problems.

Step 4 Click **Clear** to remove the contents of the Switch Health Analysis window.

Step 5 Click **Close** to close the window.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Analyzing End-to-End Connectivity

You can use the End to End Connectivity option to determine connectivity and routes among devices with the switch fabric. The connectivity tool checks to see that every pair of end devices can talk to each other, using a Ping test and by determining if they are in the same VSAN or in the same active zone. This option uses versions of the **ping** and **traceroute** commands modified for Fibre Channel networks.

To use this option, follow these steps:

Step 1 Choose **Tools > End to End Connectivity** from the Fabric Manager menu bar.

The End to End Connectivity window is displayed.

Step 2 Select the VSAN in which you want to verify connectivity from the VSAN dropdown list.

Step 3 Identify any latency issues in the network fabric by clicking the option **Report average latencies greater than** and entering the number of microseconds.

Step 4 Click **Ensure that members can communicate** to perform a Fibre Channel ping between the selected end points.

Step 5 Identify the number of packets, the size of each packet, and the timeout in milliseconds.

Step 6 Analyze the redundant paths between endpoints by clicking **Ensure that redundant paths exist between members**.

Step 7 Click **Analyze**.

The End to End Connectivity Analysis window displays the selected end points with the switch to which each is attached, and the source and target ports used to connect it.

The output shows all the requests which have failed. The possible descriptions are:

- Ignoring empty zone—No requests are issued for this zone.
- Ignoring zone with single member—No requests are issued for this zone.
- Source/Target are unknown—No nameserver entries exist for the ports or we have not discovered the port during discovery.
- Both devices are on the same switch.
- No paths exist between the two devices.
- VSAN does not have an active zone set and the default zone is denied.
- Average time ... micro secs—The latency value was more than the threshold supplied.

Step 8 Click **Clear** to remove the contents of the window.

Step 9 Click **Close** to close the window.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Analyzing Switch Fabric Configuration

The Fabric Configuration option lets you analyze the configuration of a switch by comparing the current configuration to a specific switch or to a policy file. You can save a switch configuration to a file and then compare all switches against the configuration in the file.

To use the Fabric Configuration option to analyze the configuration of a switch, follow these steps:

Step 1 Click **Fabric Configuration** from the Fabric Manager **Tools** menu.

The Fabric Configuration window is displayed.

Step 2 Choose if you want to compare the selected switch to another switch or to a Policy File.

- If you are making a switch comparison, click **Switch** and then click the drop-down arrow to see a list of switches.
- If you are making a policy comparison, click **Policy File**. Then the button to the right of this option to browse your file system and select a policy file (*.XML).

Step 3 Click **Rules** to set the rules to apply when running the Fabric Configuration Analysis tool.

The Rules window is displayed.

Step 4 Change the default rules as required and click **OK**.

Step 5 Click **Compare**.

The system analyzes the configuration and displays issues that arise as a result of the comparison.

Step 6 Click to place a checkmark in the Resolve column for the issues you want to resolve.

Step 7 Resolve them by selecting the Resolve Issues option.

Step 8 Click **Clear** to remove the contents of the window.

Step 9 Click **Close** to close the window.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Analyzing the Results of Merging Zones

You can use the Zone Merge option on the Fabric Manager Tools menu to determine if two connected switches have compatible zone configurations.

To use the Zone Merge option, follow these steps:

Step 1 Choose **Zone Merge** from the Fabric Manager Tools menu.

The Zone Merge Analysis window is displayed.

Step 2 Select a switch from each pull-down list.

Step 3 Identify the VSAN for which you want to perform the zone merge analysis.

Step 4 Click **Analyze**.

The Zone Merge Analysis window displays any inconsistencies between the zone configuration of the two selected switches.

Step 5 Click **Clear** to remove the contents of the window.

Step 6 Click **Close** to close the window.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Issuing the Show Tech Support Command

You can issue a **show tech support** command from Fabric Manager for one or more switches in a fabric. The results of each command are written to a text file, one file per switch, in a directory you specify. You can then view these files using Fabric Manager.

You can also save the Fabric Manager map as a JPG file. The file is saved with the name of the seed switch (for example, 172.22.94.250.jpg).

You can zip up all the files (the **show tech support** output and the map file image) and send the resulting zipped file to technical support.

To use the Fabric Manager **show tech support** command, perform the following steps.

Step 1 Select **Show Tech Support** from the Tools menu.

The Show Tech Support dialog box is displayed.

Step 2 Select the switches for which you want to view Show Tech Support information, by checking the checkboxes next to their IP addresses.

Step 3 Select the directory where you want the text files (containing the Show Tech Support information) to be written.

Step 4 Enter your username and password in the appropriate fields.

Note that in order for Fabric Manager to successfully issue the show tech support command on a switch, that switch must have this username and password. Fabric Manager will be unable to log into a switch that does not have this username and password, and an error will be returned for that switch.

Step 5 Set the timeout value.

The default is 30 seconds.

Step 6 Check the SSH checkbox if you want to use SSH to connect to the switch.

If you do not check the SSH checkbox, Telnet is used. Note that SSH is slower than Telnet, so if you are using SSH you may want to increase the timeout value described in Step5.

Step 7 Click the **OK** button to start issuing the **show tech support** command to the switches you specified, or click the **Close** button to close the Show Tech Support dialog box without issuing the **show tech support** command.

In the Status column next to each switch, a highlighted status is displayed. A yellow highlight indicates that the Show Tech Support command is currently running on that switch. A red highlight indicates an error. A green highlight indicates that the Show Tech Support command has completed successfully. On successful completion, a button becomes available in the View column for each switch.

Step 8 To view the Show Tech Support output, click the button next to the name of the switch. The Show Tech Support information is displayed in your default text editor.

Note If you would like to view the Show Tech Support files without using Fabric Manager, you can open them with any text editor. Each file is named with the switch's IP address and has a .TXT extension (for example, 111.22.33.444.txt).

Using Traceroute and Other Troubleshooting Tools

You can use the following options on the Tools menu to verify connectivity to a selected object or to open other management tools:

- Traceroute—Verify connectivity between two end devices that are currently selected on the Map pane.
- Device Manager— Launch the Device Manager for the switch selected on the Map pane.
- Command Line Interface—Open a Telnet or SSH session for the switch selected on the Map pane.

To use the Traceroute option to verify connectivity, follow these steps:

Step 1 Select two or more endpoints on the Fabric Manager map.

Step 2 Click **Traceroute** from the Tools menu, or right-click one of the endpoints and click **Trace Route** from the pop-up menu.

The Traceroute window is displayed.

Step 3 Change the timeout value if the default (10 seconds) is too short or too long.

Step 4 Click **Start**.

The results of the Traceroute operation appear in the Results box.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Locating Other Switches

The Locate Switches option uses SNMPv2 and discovers devices responding to SNMP requests with the read-only community string *public*. To enable your Cisco MDS 9000 Family switches to respond to SNMPv2 requests, see Chapter 10, "Managing Administrator Access."

To locate switches that are not included in the currently discovered fabric, follow these steps:

Step 1 Choose **File > Locate Switches** from the Fabric Manager main window.

You see the Locate Switches dialog box.

Step 2 Enter a range of specific addresses belonging to a specific subnet which limit the research for the switches. To look for a Cisco MDS 9000 switch belonging to subnet 192.168.199.0, use the following string:

192.168.100.[1-254]

Multiple ranges can be specified, separated by commas. For example, to look for all the devices in the two subnets 192.168.199.0 and 192.169.100.0, use the following string:

192.168.100.[1-254], 192.169.100.[1-254]

Step 3 Enter the appropriate read community string in the Read Community field.

The default value for this string is “public.”

Step 4 Click **Display Cisco MDS 9000Only** to display only the Cisco MDS 9000 Family switches in your network fabric.

Step 5 Click **Search** to discover switches and devices in your network fabric. You see the results of the discovery in the Locate Switches window.

Note The number in the lower left corner of the screen increments as the device locator attempts to discover the devices in your network fabric. When the discovery process is complete, the number indicates the number of rows displayed.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

CHAPTER 15

Troubleshooting Fabric Manager Issues

The following sections contain some common problems you may experience while using Cisco Fabric Manager, and provides solutions.

Can I Set the Map Layout So It Stays After I Restart Fabric Manager?

If you have arranged the map to your liking and would like to "freeze" the map so that the objects stay as they are even after you stop Fabric Manager and restart it again, do the following:

Step 1 Right-click on a blank space in the map. A menu is displayed.

Step 2 Select Layout -> Fix All Nodes from the menu.

Two Switches Show on my Map, But I Only Have One Switch

If two switches show on your map, but you only have one switch, it may be that you have two switches in a non-contiguous VSAN have the same Domain ID. Fabric Manager uses <vsanId><domainId> to look up a switch, and this can cause the fabric discovery to assign links incorrectly between these errant switches.

The workaround is to verify that all switches use unique domain IDs within the same VSAN in a physically connected fabric. (The fabric config checker will do this task.)

There is a Red Line Through the Switch. What's Wrong?

If a red line shows through your switch, this means Fabric Manger sees something wrong with the switch. Check the Switch->Inventory report. A module, fan, or power supply has failed or is offline and plugged in.

There is a Dotted Orange Line Through the Switch. What's Wrong?

If a dotted orange line shows through your switch, this indicates a minor status warning for that switch. Usually it means an issue with one of the modules. The tooltip should say exactly what is wrong. Hold the mouse over the switch to see the tooltip.

Can I Upgrade Without Losing My Map Settings?

When you upgrade from one version of Fabric Manager to another, there is a way to prevent the loss of map settings (enclosure names, placement on the map, etc.)

The $HOME/.cisco_mds9000/db directory contains all discovered fabrics (*.dat) and maps (*.map). These are upgradable between 1.1 and 1.2. If you need to clear the fabric cache, you should first export the enclosures to a file to avoid losing them. Everything else aside from enclosures and map coordinates are stored on the switch. The preferences, last opened, and site_ouis.txt format doesn't change from release to release.

Are There Any Restrictions When Using Fabric Manager Across FCIP?

Fabric Manager will work with no restriction across an FCIP tunnel, as long as the tunnel is up. However, Fabric Manager cannot automatically discover a Cisco SN5428 mgmt ip address in the fabric. For that switch, it will display a red slash through an FCIP device because of a timeout error. It will still see all targets, initiators, and ISLs attached to a Cisco SN5428 (or any other switch) as long as they appear in the name server or FSPF.

To work around this, you can manually enter the IP address in the Switches table, and click Apply. If the community string is correct, the red slash will go away. Even if the community string is incorrect, double-clicking on the Cisco SN5428 will launch the web tool.

Running Cisco Fabric Manager with Multiple Interfaces

If your PC has multiple interfaces (NICs), the four Cisco Fabric Manager applications detect these interfaces automatically (ignoring loopback interfaces). Fabric Manager Client and Device Manager detect all interfaces on your PC each time you launch them, and allow you to select one. Fabric Manager Server and Performance Manager detect on initial install, and allows you to select one. You are not prompted again to choose an interface with these two applications.

There may be circumstances where you will want to change the interface you are using. For example:

- If you add an interface after you have installed Fabric Manager Server and/or Performance Manager
- If you decide to use a different interface than the one you initially selected
- If for any reason one of the Cisco Fabric Manager applications did not detect multiple interfaces

Refer to the following sections, depending on which application you want to recognize the interface.

Specifying an Interface for Fabric Manager Server

To specify an interface for Fabric Manager Server, perform the following steps:

Step 1 Go to the .cisco_mds9000 folder.

Step 2 Edit the server.properties file with a text editor.

Step 3 Scroll until you find the line **snmp.localaddress**

Step 4 If the line is commented, remove the comment character.

Step 5 Set this value to the IP address or interface name of the NIC you want to use.

Step 6 Save the file.

Step 7 Stop and restart Fabric Manager Server.

Specifying an Interface for Performance Manager

To specify an interface for Performance Manager, perform the following steps:

Step 1 Go to the .cisco_mds9000 folder.

Step 2 Edit the PMCollector.conf file with a text editor.

Step 3 Scroll until you find the line **wrapper.java.additional.2=-Dmds.nmsAddress=**

Step 4 If the line is commented, remove the comment character.

Step 5 Set this value to the IP address or interface name of the NIC you want to use.

Step 6 Save the file.

Step 7 Stop and restart Performance Server.

Specifying an Interface for Fabric Manager Client or Device Manager

To specify an interface for the Fabric Manager Client or Device Manager, perform the following steps:

Step 1 Go to the .cisco_mds9000/bin folder.

Step 2 Edit the DeviceManager.bat file or the FabricManager.bat file.

Step 3 Scroll to the line that begins with set **JVMARGS=**

Step 4 Add the parameter **-Dmds.nmsaddress=ADDRESS**, where **ADDRESS** is the IP address or interface name of the NIC you want to use.

Step 5 Save the file and relaunch Fabric Manager Client or Device Manager.

Configuring a Proxy Server

If your network uses a proxy server for HTTP requests, make sure the Java Web Start Application Manager is properly configured with the IP address of your proxy server. To configure a proxy server in the Java Web Start Application Manager, follow these steps:

Step 1 Double-click the Java Web Start application manager icon on your Windows desktop, or Chose **Program Files > Java Web Start**.

Step 2 Select **File > Preferences** from the Java WebStart Application Manager.

Step 3 Click the **Manual** radio button and enter the IP address of the proxy server in the HTTP Proxy field.

Step 4 Enter the HTTP port number used by your proxy service in the HTTP Port field.

Step 5 Click **OK**.

CHAPTER 16

Managing Advanced Features

Cisco MDS 9000 Family switches support advanced features, such as world wide names, domains, and name server. The Fabric Manager allows you to configure these features on multiple Cisco MDS 9000 switches. The Device Manager allows you to configure these features on a single Cisco MDS 9000 switch.

Note For information about configuring these advanced features using the command-line interface (CLI), refer to the *Cisco 9000 Family Configuration Guide*.

Procedures for managing advanced features include:

Managing World Wide Names

Each port on a Cisco MDS 9000 Family switch is uniquely identified by its world wide names (WWNs), which include the switch MAC address and an identifier for each port. The principal switch selection and the allocation of domain IDs use the WWN to identify a specific port.

To add WWNs, perform the following steps.

Step 1 From the Fabric Manager, choose **FC > WWN Manager** on the menu tree, OR
From the Device Manager, choose **WWN Manager** from the FC menu.

The information pane of the Fabric Manager displays WWN information for multiple switches. The dialog box from the Device Manager displays WWN information for a single switch.

Step 2 Configure the BaseMacAddress and MacAddressRange attributes for the WWN(s).

Step 3 In the Fabric Manager information pane, the information is updated. In the Device Manager dialog, click Apply to accept the changes; click Close to close the WWWN Manager dialog without saving changes.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Managing Domain Parameters

Procedures for managing domain parameters include:

Managing Running Attributes for Domains

To view running domain attributes from the Fabric Manager, choose **FC > Domain Manager** on the menu tree and click the **Running** tab. The Information pane from the Fabric Manager displays domain attributes for multiple switches.

To view running domain attributes from the Device Manager, choose **Domain Manager** from the FC menu and click the **Running** tab. The Domain Manager dialog box, with the Running tab selected, displays domain attributes for a single switch.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Configuring Domain Attributes

From this dialog box you can specify a fabric name for fabric logins on the VSAN and set the priority for the switch used in the principal switch selection process.

Configure the principal attributes for the domain.

To manage domain attributes from the Fabric Manager, choose **FC > Domain Manager** on the menu tree and click the **Configuration** tab. The Information pane from the Fabric Manager lets you manage domain attributes for multiple switches.

To manage domain attributes from the Device Manager, choose **Domain Manager** from the FC menu and click the **Configuration** tab. The Device Manager dialog box displays domain attributes for a single switch.

Configure the attributes for the domain.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Viewing Domain Information

To view domain information from the Device Manager, choose **Domain Manager** from the FC menu and click the **Domains** tab. The dialog box displays domain information for a single switch

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Viewing Domain Manager Statistics

To monitor domain manager statistics from the Fabric Manager, choose **FC > Domain Manager** on the menu tree and click the **Statistics** tab. The Information pane from the Fabric Manager displays domain statistics for multiple switches.

To monitor domain manager statistics from the Device Manager, choose **Domain Manager** from the FC menu and click the **Statistics** tab. The Domain Manager dialog box, with the **Statistics** tab selected, displays domain statistics for a single switch.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Configuring Domain Interfaces

To configure domain interfaces from the Fabric Manager, choose **FC > Domain Manager** on the menu tree and click the **Interfaces** tab. The Information pane from the Fabric Manager displays domain interfaces for multiple switches.

To configure domain interfaces from the Device Manager, choose **Domain Manager** from the FC menu and click the **Interfaces** tab. The Domain Manager dialog box, with the Interfaces tab selected, displays domain interfaces for a single switch.

Configure the attributes for domain interfaces.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Viewing Domain Areas

To monitor domain areas from the Device Manager, choose **Domain Manager** from the FC menu and click the **Areas** tab. The Domain Manager dialog box, with the Areas tab selected, displays domain areas for a single switch.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Configuring Persistent FCIDs

By default, the persistent FC_ID feature is disabled. When a N/NL-port logs into a switch, and gets assigned an FC ID, the WWN of the requesting N/NL-port and the assigned FC ID is retained and stored in a volatile cache (the content is lost after a reboot).

If the persistent FC ID feature is disabled, binding of the FC ID to the WWN is preserved on a best effort basis.

For example, after the disconnection of one N-Port from the switch, if its FC ID is requested by another device, the request is granted and the initial association WWN FC ID is released. Also, if the 4K entries of the volatile cache used to store the WWN-to- FC ID binding get completely filled up, a new (more recent) entry will overwrite the oldest one, losing the corresponding binding WWN to FC ID.

The behavior is different for an N-Port than for an NL-Port:

- N-ports should receive the same FC IDs if unplugged and plugged back in any port of the same switch (as long as it belongs to the same VSAN)
- NL-port should receive the same FC IDs only if connected back to the same interface on the switch it was connected originally.

The assigned FC IDs in a fcdomain can be activated to remain persistent, even after a reboot. This ensures that an attached N Port receives the same FC ID after a switch reboot. If you enable this feature, the following apply:

- The currently “in-use” FC IDs in the fcdomain will be saved across reboots.
- The fcdomain automatically populates the database with dynamic entries that the switch has learned about after a device (host or disk) is plugged into a port interface.

To configure persistent FCIDs from the Fabric Manager, choose **FC > Domain Manager** on the menu tree and click the **Persistent FCIDs** tab. The Information pane from the Fabric Manager displays persistent FCIDs for multiple switches.

To configure persistent FCIDs from the Device Manager, choose **Domain Manager** from the FC menu and click the **Persistent FCIDs** tab. The Domain Manager dialog box, with the Persistent FCIDs tab selected, displays persistent FCIDs for a single switch.

Configure the attributes for persistent FCIDs.

Before you can create persistent FCIDs, you must:

- Configure a static domain ID in that VSAN
- Ascertain that the static configured domain and the runtime domain are the same. You can verify this using the show fcdomain command. For information about using the command line interface (CLI), refer to the *Cisco 9000 Family Configuration Guide*.

Note If you connect to the switch from an AIX or HP-UX host, be sure to create the persistent FC ID in the VSAN that connects these hosts.

Note Persistent FC IDs with loop-attache devices (FL ports) need to remain connected to the same port in which they were configured.

To create a new persistent FCID, do the following:

Step 1 Click the Create button.

The Create Domain Manager Persistent FCIDs dialog is displayed.

Step 2 Enter the VSAN ID.

Step 3 Enter the WWN.

Step 4 Enter the FCID.

Step 5 Select the Mask.

This is the number of FC IDs which are assigned either statically or dynamically for this WWN on this VSAN. Possible values are Single, meaning just one FCI ID is assigned, or Area, meaning all of the FC IDs in the area that is specified are assigned.

Step 6 Select the Assignment.

This is the type of persistency of this FC ID (static or dynamic).

Step 7 Click Create to create the persistent FCID; click Close to return to the Domain Manager without creating the FCID.

To delete a persistent FCID, do the following.

Step 1 Select the persistent FCID you want to delete.

The Delete button is enabled.

Step 2 Click the Delete button to delete the FCID.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Viewing Domain Area Ports

To monitor area ports for domains from the Device Manager, choose **Domain Manager** from the FC menu and click the **Area Ports** tab. The Domain Manager dialog box, with the Area Ports tab, displays area ports for domains for a single switch.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Configuring the Name Server

Configuring the Name Server includes the following tasks.

Viewing General Attributes for the Name Server

To view general name server attributes from the Device Manager, choose **Name Server** from the FC menu. The Name Server dialog box, with the General tab selected, displays name server attributes for a single switch.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Viewing Advanced Attributes for the Name Server

To monitor advanced name server attributes from the Device Manager, choose **Name Server** from the FC menu and click the **Advanced** tab. The Name Server dialog box, with the Advanced tab selected, displays advanced name server attributes for a single switch.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Proxy Ports for the Name Server

To configure proxy ports for the name server from Fabric Manager, choose **FC > Name Server** on the menu tree and click the **Proxies** tab. The Information pane from the Fabric Manager displays name server proxy ports for multiple switches.

To configure proxy ports for the name server from the Device Manager, choose **Name Server** from the FC menu and click the **Proxy** tab. The Name Server dialog box, with the Proxy tab selected, displays name server proxies for a single switch.

Configure proxy attributes for the name server.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Viewing Name Server Statistics

To monitor name server statistics from the Fabric Manager, choose **FC > Name Server** on the menu tree and click the **Statistics** tab. The Information pane from the Fabric Manager displays name server statistics for multiple switches.

To monitor name server statistics from the Device Manager, choose **Name Server** from the FC menu and click the **Statistics** tab. The Name Server dialog box, with the Statistics tab selected, displays name server statistics for a single switch.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Viewing LUN Information

This section describes how to manage LUN information and includes the following topics:

Configuring LUN Discovery

To view logical unit number (LUN) information from the Device Manager, choose **LUN** from the FC menu.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Viewing Logical Unit Information

To view logical unit number (LUN) information from the Device Manager, choose **LUN** from the FC menu and click the **Logical Units** tab.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Viewing LUNs Information

To view LUNs information from the Device Manager, choose **LUN** from the FC menu and click the **LUNs** tab.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Viewing RSCN Information

This section describes how to view RSCN information and includes the following topics:

Viewing RSCN Nx Registrations

To view Nx registrations for RSCN from the Fabric Manager, choose **FC > RSCN** on the menu tree, and click the **Registrations** tab. The Information pane from the Fabric Manager displays Nx registrations for RSCN for multiple switches.

To monitor Nx registrations for RSCN from the Device Manager, choose **RSCN** from the FC menu. The RSCN dialog box, with the Nx Registrations tab selected, displays Nx registrations for RSCN for a single switch.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Viewing RSCN Statistics

To monitor registered state change notification (RSCN) statistics from the Fabric Manager, choose **FC > RSCN** on the menu tree and click the **Statistics** tab. The Information pane from the Fabric Manager displays RSCN statistics for multiple switches.

To monitor RSCN from the Device Manager, choose **RSCN** from the FC menu and click the **Statistics** tab. The RSCN dialog box, with the Statistics tab selected, displays RSCN statistics for a single switch.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Configuring Timers

To configure timers from the Fabric Manager, choose **FC > Timers & Policies** on the menu tree. The Information pane from the Fabric Manager displays timers for multiple switches.

To configure timers from the Device Manager, choose **Timers/Policies** from the FC menu. The dialog box from the Device Manager displays timers for a single switch.

Configure the timer attributes.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Configuring Virtual Routing Redundancy Protocol (VRRP)

Cisco MDS 9000 Family switches support the Virtual Router Redundancy Protocol (VRRP), as described in RFC 2338. VRRP provides redundant paths to a gateway switch. For further information about VRRP, refer to the *Cisco MDS 9000 Family Configuration Guide*.

This section describes how to use Device Manager to configure VRRP and includes the following information:

Configuring VRRP Operations Attributes

To configure VRRP operations attributes from Device Manager, choose **VRRP** option from the IP menu. The VRRP dialog box with the Operations tab selected is displayed.

Configure Operations attributes for the virtual router.

To create a new VRRP entry, click the **Create** button. You see the Create VRRP Entry window.

Complete the fields on this window to create a new VRRP entry, and click **OK** or **Apply**.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Managing IP Addresses for VRRP

To manage IP addresses for virtual routers from Device Manager, click the **IP Addresses** tab on the VRRP dialog box.

The VRRP dialog box with the IP Addresses tab selected is displayed.

To create a new VRRP entry, click the **Create** button. You see the Create VRRP IP Addresses window.

Complete the fields on this window to create a new VRRP IP Address, and click **OK** or **Apply**.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Viewing VRRP Statistics

To monitor VRRP statistics, click the **Statistics** tab on the VRRP dialog box. The VRRP dialog box with the Statistics tab selected is displayed.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Managing Fibre Channel Routing and FSPF

Fabric Shortest Path First (FSPF) is the standard path selection process used by Fibre Channel fabrics. FSPF automatically calculates the best path between any two switches in the fabric. All routes across the fabric are established when switches are powered up. These routes do not change unless there is a failure or unless a new ISL (or EISL) is created that offers a path equal to or better than an existing path.

The Fabric Manager allows you to configure and monitor these routing services on multiple Cisco 9000 switches. The Device Manager allows you to configure and monitor Fibre Channel routing and FSPF on a single Cisco 9000 switch. For information about Fibre Channel routing and how to configure routing and FSPF using the command line interface (CLI), refer to the *Cisco 9000 Family Configuration Guide*.

Procedures for configuring Fibre Channel Routing include:

Procedures for configuring FSPF include:

Configuring Fibre Channel Routes

To configure Fibre Channel routes, do the following:

Step 1 From the Device Manager, choose **Routes** from the FC menu. The dialog box displays routes for a single switch.

Step 2 Configure the attributes for the route.

Step 3 To add a route from Device Manager, click **Create** on the dialog box.

You see the Create Route dialog box.

Step 4 Click the button to the right of the Interface field and select the interface on which to configure the Fibre Channel route.

Step 5 Complete the other fields on this window and click **OK** to add a route.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Configuring Fibre Channel Route Flows

To view Fibre Channel flows, do the following:

Step 1 From the Fabric Manager, choose **FC > Route Flow Statistics** on the menu tree. The Information pane from Fabric Manager displays flows for multiple switches.

From the Device View, choose **Routes** from the FC menu and click the **Flow Statistics** tab. The dialog box from the Device Manager displays flows for a single switch.

Step 2 Configure the flow attributes for the route.

Step 3 To add a route flow from Fabric Manager, click **Create Row** on the toolbar.

To add a route flow from Device Manager, click **Create** on the dialog box.

The Create Route flow dialog is displayed.

Step 4 Complete the fields on this window and click **Create** to add a route flow.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Managing FSPF General Attributes

To manage FSPF general attributes, do the following:

Step 1 From the Fabric Manager, choose **FC > FSPF** on the menu tree and click the **General** tab.

From the Device Manager, choose **FSPF** from the FC menu and click the **General** tab.

The Information pane from the Fabric Manager displays information for multiple switches. The dialog box from the Device Manager displays FSPF information for a single switch.

Step 2 Configure the FSPF general attributes.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Configuring FSPF Interfaces

To configure FSPF interfaces, do the following:

Step 1 From the Fabric Manager, choose **FC > FSPF** on the menu tree and click the **Interfaces** tab.

To configure FSPF interfaces from the Device Manager, choose **FSPF** from the FC menu and click the **Interfaces** tab.

Step 2 Configure the attributes for the FSPF interfaces.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Viewing FSPF Statistics

To monitor FSPF statistics from the Fabric Manager, choose **FC > FSPF** on the menu tree and click the **Statistics** tab.

To monitor FSPF statistics from the Device Manager, choose **FSPF** from the FC menu and click the **Statistics** tab.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Viewing FSPF Interface Statistics

To monitor FSPF interface statistics from the Fabric Manager, choose **FC > FSPF** on the menu tree and click the **Interface Stats** tab.

To monitor FSPF interface statistics from the Device Manager, choose **FSPF** from the FC menu and click the **Interface Stats** tab.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Viewing Link State Records

To monitor FSPF LSRs from the Device Manager, choose **FSPF** from the FC menu and click the **LSDB LSRs** tab.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Viewing FSPF Links

To view FSPF links from the Device Manager, choose **FSPF** from the FC menu and click the **LSDB Links** tab.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Managing SPAN

You can configure SPAN sessions using Device Manager. Each SPAN session represents an association of one destination with a set of source(s). The sources can be FC ports or the supervisor's FC0 port, and the destination can be either an FC port or an FCIP tunnel. You can configure up to 16 SPAN sessions in a switch.

The list below shows the SPAN tasks you can perform with Device Manager. SPAN is not configurable from Fabric Manager.

- Creating SPAN Sessions, page 16-13
- Editing SPAN Sources, page 16-13
- Deleting SPAN Sessions, page 16-14

Creating SPAN Sessions

To create a SPAN session, perform the following steps.

Step 1 From the Device Manager, choose **SPAN** from the **Interface** menu.

The SPAN dialog box is displayed.

Step 2 Select the **Sessions** tab.

Step 3 Click the **Create** button.

The Create SPAN Session dialog is displayed.

Step 4 Select the session ID (from 1-16) using the up or down arrows, and click the **Create** button.

Step 5 Repeat Step 4 for each session you want to create.

Step 6 Click the **Close** button to close the Create SPAN Session dialog.

Step 7 Specify the destination interface by clicking once in the **Dest Interface** field for the appropriate session.

Step 8 Specify the filter VSAN list by clicking once in the Filter VSAN List field for the appropriate session.

Step 9 Choose **active** or **inactive** admin status by clicking the Admin dropdown menu and selecting the appropriate status.

Step 10 Click the **Apply** button to save your changes, or click the **Close** button to close the SPAN Sessions dialog without saving your changes.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Editing SPAN Sources

To edit a SPAN source, perform the following steps.

Step 1 From the Device Manager, choose **SPAN** from the **Interface** menu.

The SPAN dialog box is displayed.

Step 2 Select the **Sources** tab.

Step 3 Click once on the **VSAN List** field, and enter the VSAN list name.

Step 4 Click on the Edit FC Source button.

The Edit FC Interface Source dialog box is displayed.

Step 5 Click the **Create** button.

The Create FC Interface Source dialog is displayed.

Step 6 Click the **...** button to display the list of available FC ports. Select a port and click OK.

Step 7 Click the direction (**receive** or **transmit**) you want.

Step 8 Click the **Create** button to create the FC interface source, or click the **Close** button to close the Create FC Interface Source dialog without creating the interface source.

Step 9 Click the Close button. The new FC interface source is listed in the FC Interface Source dialog box list.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Deleting SPAN Sessions

To delete a SPAN session, perform the following steps.

Step 1 From the Device Manager, choose **SPAN** from the **Interface** menu.

The SPAN dialog box is displayed.

Step 2 Select the **Sessions** tab.

Step 3 Click once to select the SPAN session you want to delete.

Step 4 Click the **Delete** button.

The SPAN session is deleted.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

INDEX

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

X

Z